

Access Control Software User Manual

Version: 2.4.4.1038

Date: November 2010

Table of Contents

1. Install and Uninstall Software.....	1
1.1 Install Software	1
1.2 Uninstall Software.....	4
2. Department Management	5
3. User Management	9
3.1 User Fingerprint.....	9
3.2 Statistic	16
3.3 Upload and Download	20
4. Device Management.....	23
4.1 Device Information.....	25
4.2 Communication	26
4.3 Wiegand	27
4.4 Verification	30
4.5 Power Management	31
4.6 Access Control	32
4.7 Mifare	34
4.8 Other Setup	34
4.9 U disk Setting	36
5. U Disk Management	39
5.1 Import User Data	39
5.2 User Data Export.....	41
5.3 Record Data Import	42
5.4 Import Sms	42
5.5 Export the Sms Data	44
5.6 Import Photos	45
6. SMS Management.....	46


6.1 SMS Content Manage	46
6.2 Employee SMS customization	48
7. System Management.....	51
7.1 Operator Management	51
7.2 System Operation Log	52
7.3 Data Maintenance	54
7.4 Initialize System.....	54
7.5 Set Database	54
7.6 Set Password of Database	57
7.7 System Options	57
8. Access Control Setup	61
8.1 Time Zone	61
8.2 Group	63
8.3 Unlock Combination	65
8.4 Access Control Privileges	67
8.5 Holidays setting	74
8.6 Upload Setting	76
9. Other Function.....	79
9.1 Start Monitor	79
9.2 Download Log	79
9.3 Clear Log	80
9.4 Sync Time.....	80
9.5 Update Firmware	80
9.6 Restart Device	80
9.7 Property	81
9.8 Stop Sound	81
10. Record Management	82
10.1 Record Query	82

10.2 Alarm Report	84
11. Appendix	87
11.1 Common Operation	87
11.2 FP, FP device and Card User Guide	91
11.3 SOFTWARE USE LICENSE AGREEMENT	95

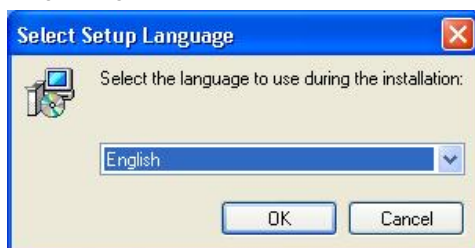
1. Install and Uninstall Software

1.1 Install Software

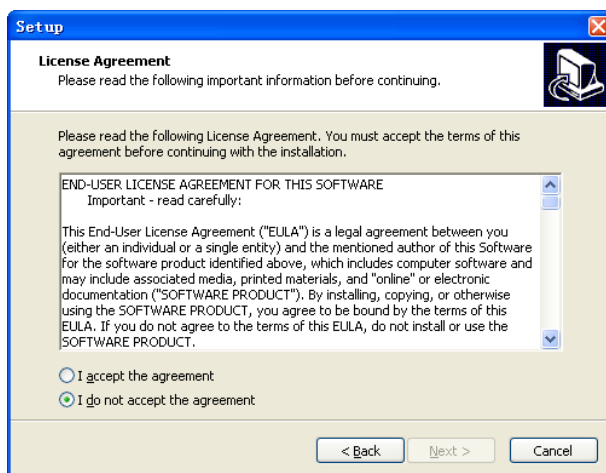
Before installing your software, it is better to shutdown all the other application programs, in order to keep away conflict in installing process.

 **Note:** The following screen may differ from what you see upon CD installation. Please refer to CD installation.

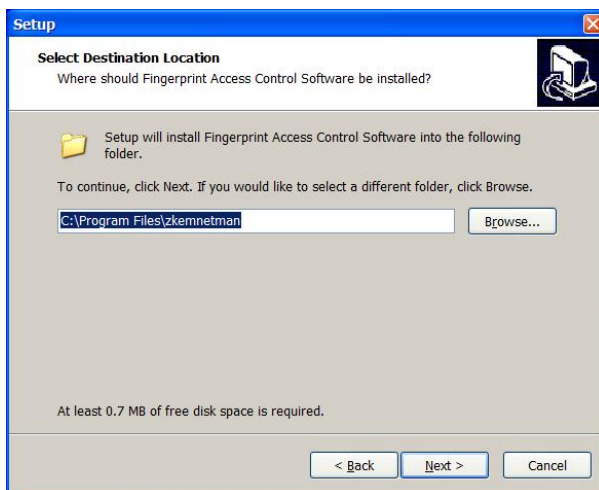
1. Please put the software CD into CD-ROM, it will run automatically and popup the following dialog.



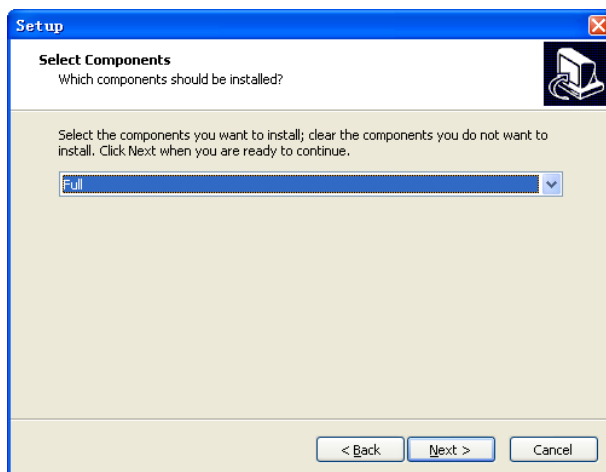
2. Select the Language, click [OK], and enter the following interface.



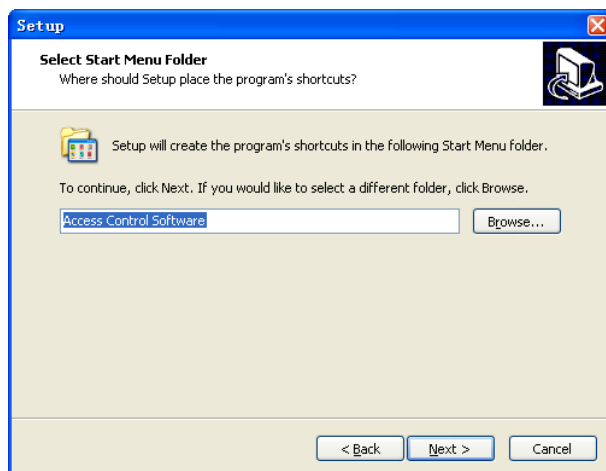
3. Please read the Agreement carefully. If you want to install please select **[I accept the agreement]**, and click **[Next]**, enter the following interface.



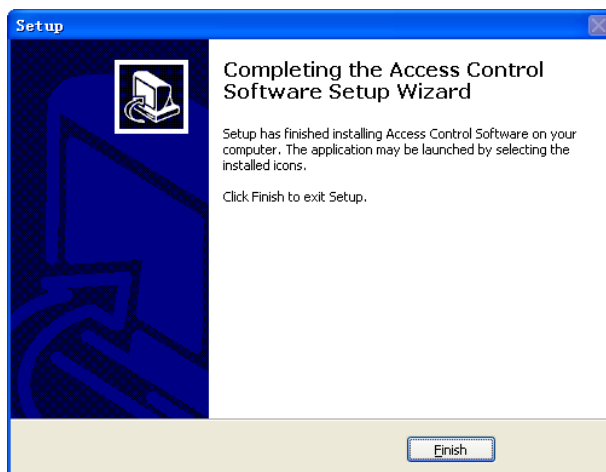
4. Select the folder where to install the software. Click **[Next]** to enter the following interface.



5. Select the install component, and click **[Next]** to continue.



6. Click **[Install]**, the installing program will copy and write corresponding information into hard disk. After finish installation, click **[Finish]** to complete the process.



1.2 Uninstall Software

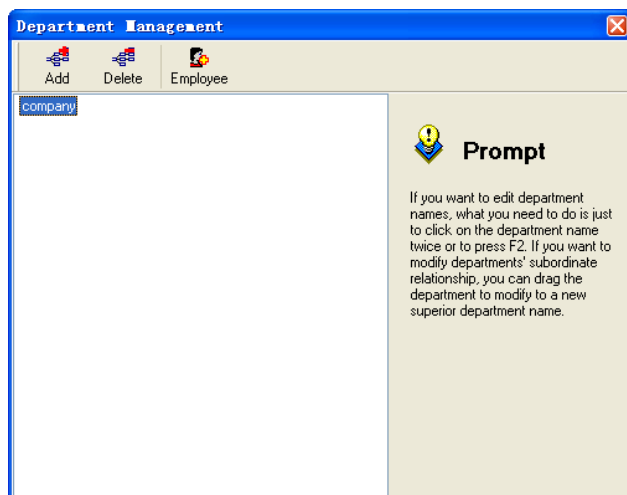
If you do not need to use this software any more, and want to uninstall it from your computer, then may follow next steps to operate:




1. Close the Access Control Software complete.
2. Enter **Start/ Control panel**.
3. Enter **Add and Cancel Program** window, choose Access Control Software, and click **[Remove]** button to uninstall.

Like doing this, you still cannot delete all files. You need enter the installation directory of the software to delete the folder where the software installed.

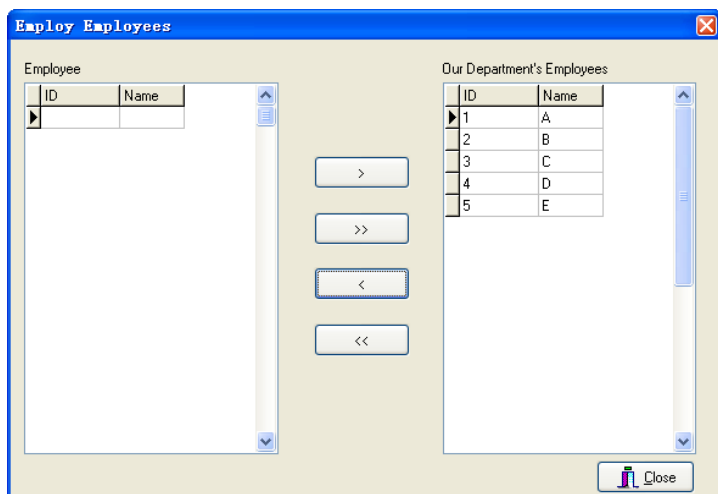
2. Department Management

Click **[Department]** in the **[Base Options]** menu, popup the Department Management main interface, like as following figure.

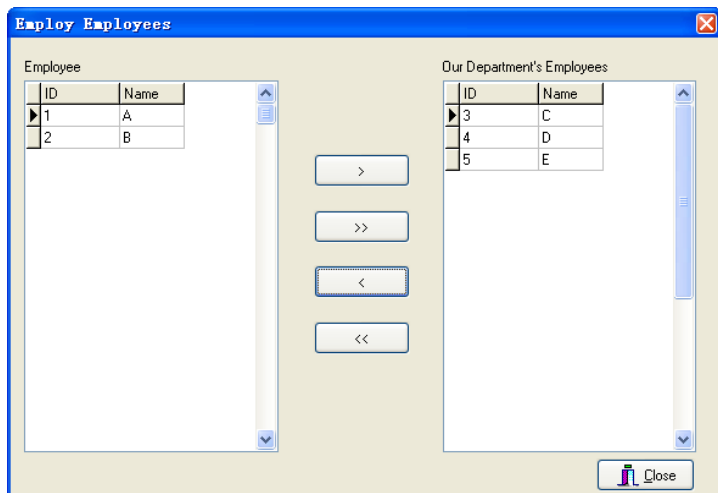


Click  or  to add or delete a department,  is **[Employee]** Button.

Employ staff to the department: First to select the name of company, then click Employee button, popup following interface.

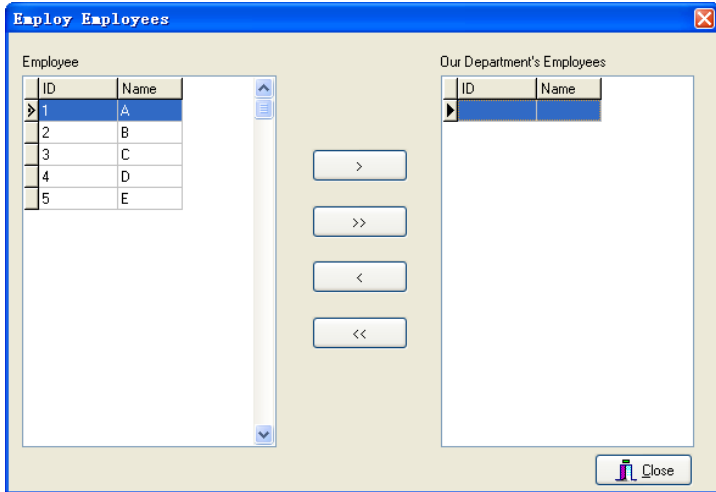


“Our Department’s Employees” box at right side is the employees list of company, first choose the employee to shift, and then click the “<” button to move the employee to the left side, or click “<<” button to move all employees to the left side.

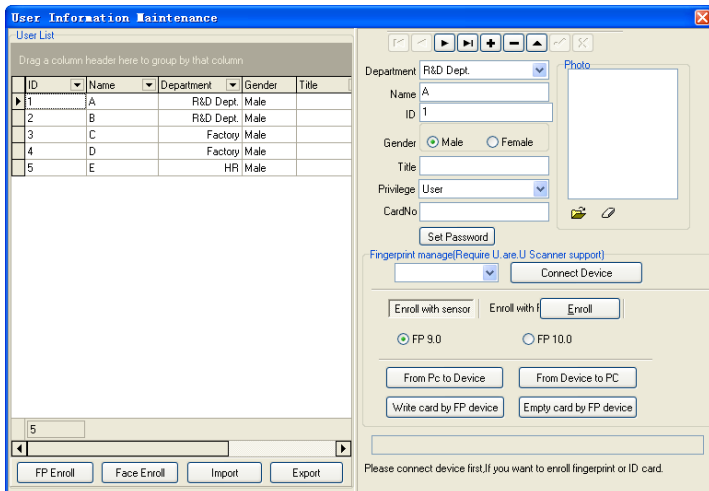


2. Department Management

Select a department, click Employee button, the interface as shown below.



Select the staff to employ, click ">" to move the staff to the right side of related department, or click ">>" button to move all employees to the right side to complete shifting the staff.



To shift a staff can directly process in the [**User Management**] interface.

3. User Management

User Management is the process to maintenance user information, click **[User Manage]** in the **[Base Options]** menu or the shortcut button, popup the User Information Maintenance interface, as following.

ID	Name	Department	Gender	Title
1	A	R&D Dept.	Male	
2	B	R&D Dept.	Male	
3	C	Factory	Male	
4	D	Factory	Male	
5	E	HR	Male	

Add User: Click button in the staff maintenance bar to add new user.

Cancel User: Choose the user you want delete, and click button to delete the user.

Photo: Click button to import user photo, or click button to delete.

3.1 User Fingerprint

1. Enroll User Fingerprint

Enroll with FP Sensor:

If you need to use the FP Sensor to enroll fingerprint, please install the FP Sensor driver program first. The driver is under the Driver directory in

software CD. After complete to install the driver, connect the FP sensor to the PC USB port. The current software version supports to use the “U are U” series, ZK4000/6000/7000 FP sensor and etc.

(1) Select **[Enroll with Sensor]** in User Information Maintenance interface, click **[Enroll]** button, and enter the fingerprint enrollment interface, as shown below.

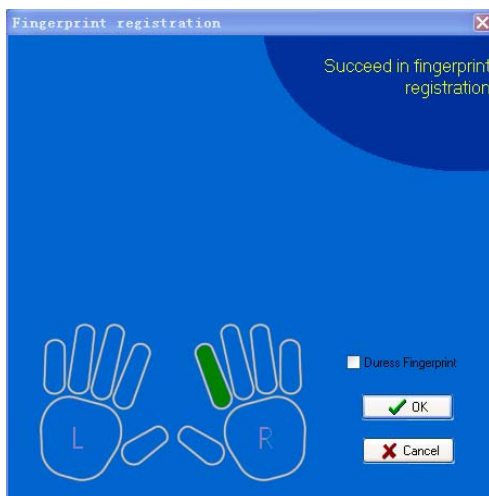


(2) Click the finger which fingerprint is to be enrolled, and the system enters the interface to enroll, as shown below:

3. User Management

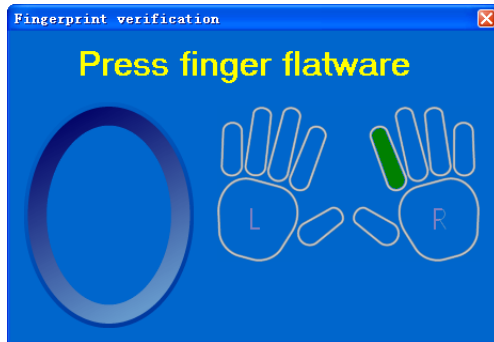


(3) After the finger finishes 3 times press on the FP Sensor, the system prompt "Succeed in fingerprint registration", shown as below.



(4) Click "OK" after successful enrollment, save the fingerprint and return to user's information maintenance interface.

(5) Click “verify”, the following interface will appear to check if the fingerprint enrollment is succeed or not.



(6) Press the enrolled finger on the sensor, the following dialog appear when the sensor collect the fingerprint, that is, fingerprint enroll succeeds.



If the following dialog appears, then the enrollment failed, please return to enroll once again.



(7) If you want to delete the fingerprint, please double click this finger, the system prompts the following:



(8) If you select [**Duress Fingerprint**], the enrolled fingerprint will be a duress fingerprint for use.


Enroll with FP Reader:

Use the FP Reader to enroll fingerprint. Select FP Reader in User management interface, click [**Connect Device**], and the [Connect] button

will turn to [Disconnect] when the connection completed. Click **[Enroll]** button, and enter the fingerprint enrollment interface. The FP reader enrollment is similar to FP sensor, except there is no verification process for FP reader.

2. Register Mifare Card:

Choose the user who need to register the Mifare Card. Click **[Through Fingerprint Reader to Write Card]**, swipe the card near to the card sensor area of the FP Reader when the software remind **“Present Card”**. If the device prompt **“Write Card Successfully”**, this user's ID and the fingerprint will store in the card. Click **[Through Fingerprint Reader to Clear Card]** to delete user's data in the Mifare, swipe the card near to the card sensor area of the FP Reader when the software remind **“Present Card”**. The notice **“Clear Card Successfully”** means the operation complete.

 **Note:** This function is available only for the FP Reader which supports Mifare card enrollment.

3. Fingerprints Enroll Status: Shows the detail of user information and fingerprint enroll status.

3. User Management

FP Enroll

Preview

Drag a column header here to group by that column

ID	Name	FP Count
1	A	0
2	B	0
3	C	0
4	D	0
5	E	0

Count 0

4. User face Enroll Status: Shows the detail of user and face enroll status.

Face Enroll

Preview

Drag a column header here to group by that column

ID	Name	Face Count
1	A	0
2	B	0
3	C	0
4	D	0
5	E	0

Count 0

5. Sort Order:

You can arrange the record according to the ascending or descending order in the record list, directly click the head of rank to achieve. Choose a triangle symbol which is beside the field, according to ascending order to arrange when the triangle symbol point upwards, otherwise that means the sort order follow the descending order. You can click the triangle symbol to change the rise or down rank.

As figure below, sort the user as the name order.

The screenshot shows the 'User Information Maintenance' window. On the left is a 'User List' table with columns: ID, Name, Department, Gender, and Title. The table contains five records. Below the table are buttons for 'FP Enroll', 'Face Enroll', 'Import', and 'Export'. On the right is a form for user details, including fields for Department, Name, ID, Gender, Title, Privilege, and CardNo. There are also buttons for 'Set Password', 'Connect Device', and enrollment options for fingerprint and face. A note at the bottom says 'Please connect device first, if you want to enroll fingerprint or ID card.'

ID	Name	Department	Gender	Title
1	A	R&D Dept.	Male	
2	B	R&D Dept.	Male	
3	C	Factory	Male	
4	D	Factory	Male	
5	E	HR	Male	

3.2 Statistic

The software can automatically count the total records and count the grouping records.

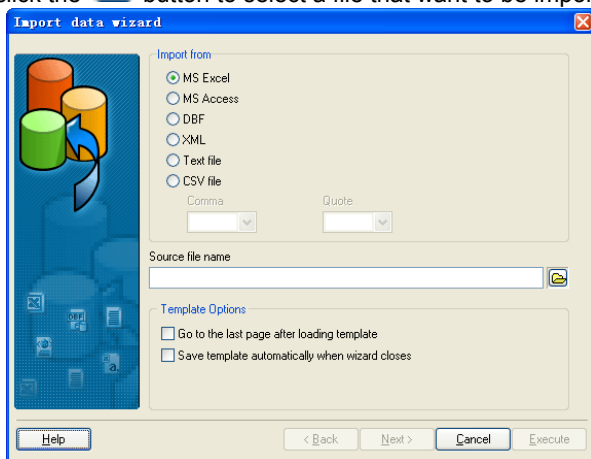
1. Import

This function enables the user to import many formats of user's data file, such as: MS Excel, MS Access, DBF, XML, Text File, CSV file. We recommend to use the CSV file to import. The following example is using

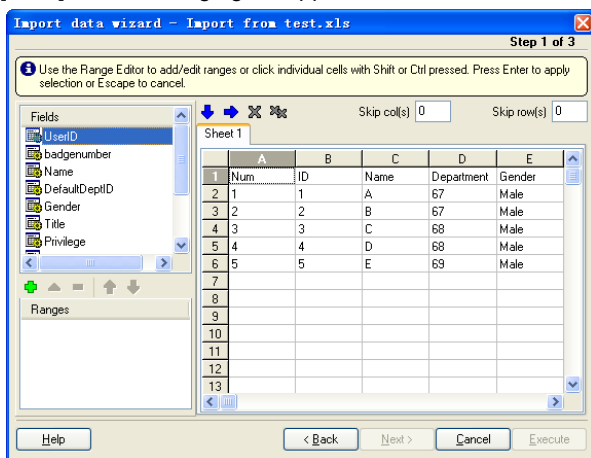
3. User Management

text file to import user's data.

- (1) First click the  button to select a file that want to be imported.



- (2) Click [Next], the following figure appears:



On the left side there is the field list, and the right side is the importing file rank. The Skipcol(s) on the right-up part means how many columns to skip, the Skiprow(s) means how many rows to skip. If the first line of the

importing file is not the material data, you can fill "1" in Skiprow(s) blank, that shows to skip the first line for importing data.

UserID: The ID is only used for system internal, it is useless for file import, please don't use it.

BadgeNumber: User code, this code is the user number used in the FP Reader and the software.

Name: User name, these fields must exist.

DefaultDeptID: Department ID. If you import the data from other sources, this item can be neglected.

Gender: Male or Female.

Title: Title.

Privilege: Privilege, can be neglected.

Password: Password, can be neglected.

CardNo: ID card number, can be neglected.

MverifyPass: The user password used in the device, can be neglected.

VerificationMethod: The verification method of user. This item can be neglected.

(3) First choose the field in the Fields list as to import, and then select the corresponding rank in the right side list. The Fields list will automatically attach the corresponding number to the name of field, such as it is, arrange all fields and corresponding rank after finish it, move to the next step.

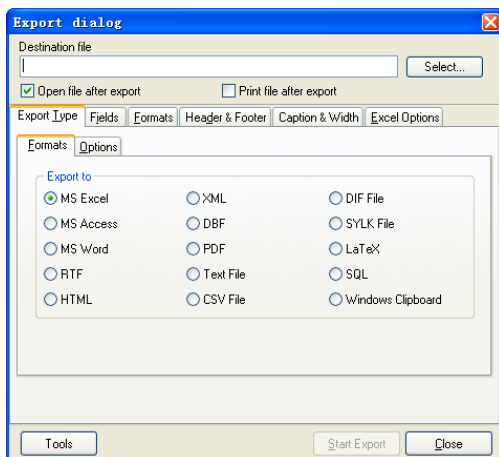
If you want to cancel a field, first choose the field, and then click corresponding rank, the software will cancel this field.

(4) Click the [**Execute**] button to run importing operation.

2. Export:

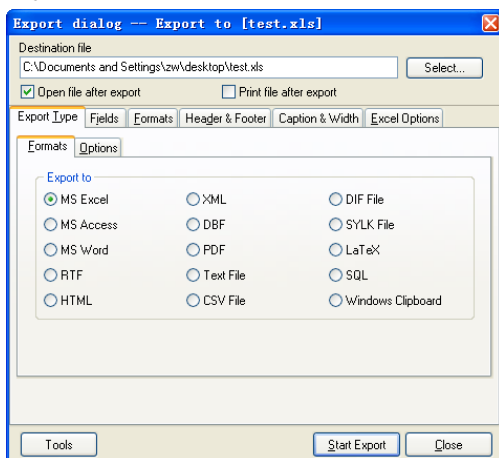
This function enables the software export user's data via all kinds of format which can be supported by the software. It is convenient to supply for third party software to use.

Click the **[Export]** button, appear following interface.



Take the exporting MS Excel file as an example to explain.

(1) Select the object file which is to be exported.



(2) Click **[Start Export]** button to export the file via default format. Otherwise, you can configure exporting content through the following option cards.

Fields: Select the field to be export, the default is all, it is only to export field's content after selecting.

Formats: The exporting format of all kinds of defined field value.

Header & Footer: The file to start and to end of the text.

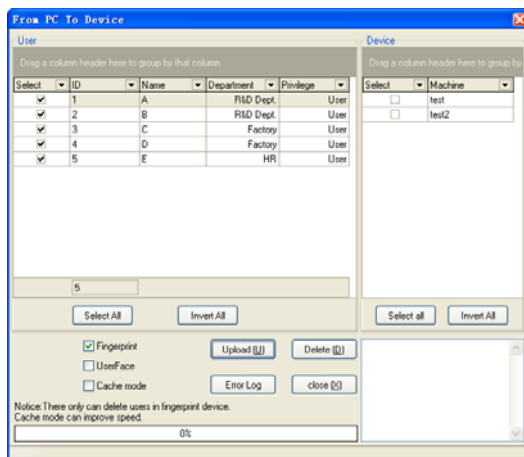
Caption & Width: The title and width of field.

Excel Options: Set font.

3.3 Upload and Download

1. From PC to Device:

The user which is store in the database will be uploaded to the FP Reader, click **[From PC to Device]**, popup the interface to upload user's data.



Upload: Based your need, select the staff and a uploading FP Reader, click **[Upload]**, it is able to upload user's data to the defined FP Reader, it is better to select **[Fingerprint]** and **[User Face]** in the normal condition. If the information needs not to be modified, it is no need to choose it.

Notice: User's data include user information, fingerprint and user face.

Delete: If you want to delete a user in a FP Reader, first choose user and

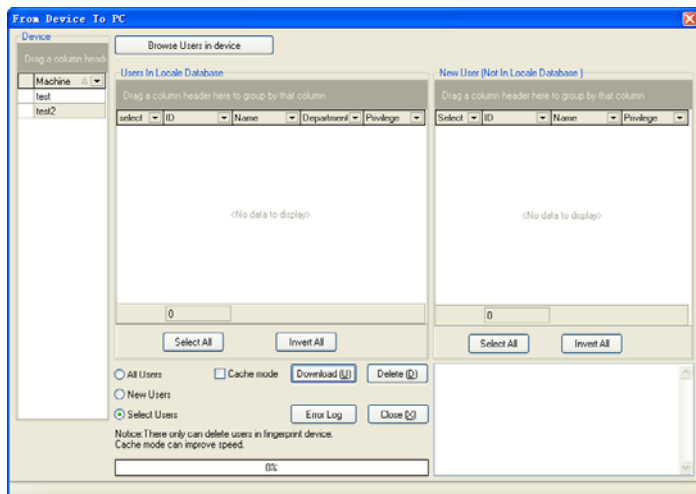
corresponding FP Reader, and then click **[Delete]** button.

Operation Log: That is an error log during operating process.

Batch: Utilize this function to speed up communication when a lot of user's data are uploaded, it needn't for a few users (such as less than 30 users).

2. From Device to PC:

Download the user data from the FP Reader to the local database. Click **[Form Device to PC]**, popup the interface to download user's data.



Select a FP Reader to download user's information which is on the left side list, click **[Browse Users in Device]**, all users in the FP Reader is displayed. Select the user to be downloaded, click the **[Download]** button to download the user data from FP Reader to local database.

View User in the Device: Display all users in the FP Reader.

Download: Download user data to be selected.

Delete: If you want to delete a user in a FP Reader, first choose user, and then click **[Delete]** button.

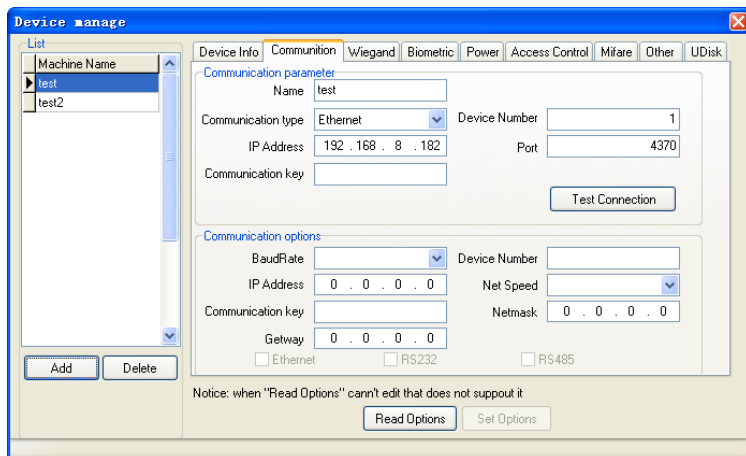
Batch: Utilize the function to speed up communication when a lot of users

are downloaded, it needn't for a few users.

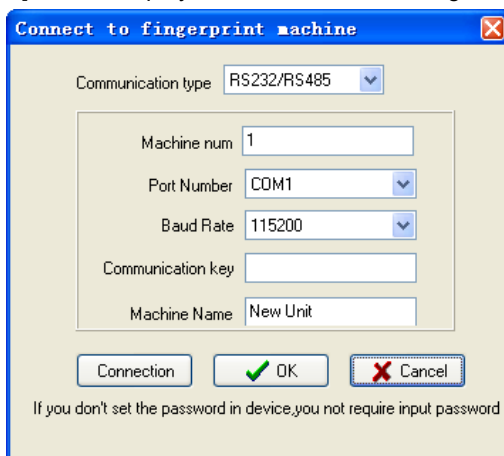
Operation Log: That is an error log during operating process.

4. Device Management

Add device: Open **[Device List]** in the **[Base Options]** menu, or click **[Device Manage]** shortcut on the main interface, and display the interface as following.



Click **[Add]** button, display the interface as following.



RS232/RS485 Communication:

Machine num: According to the Reader number to fill, for example the FP Reader number is 1.

Port: Properly select the communication port to connect PC, the default port is COM1.

Baud Rate: Select the same baud rate as the FP Reader. The default value is 38400 at its original setup.

Communication key: It isn't need to fill the pass word in the default condition, if there is a setup password in the FP Reader, please input correct password.

Machine Name: According to the purpose of device, input an observable name.

Ethernet Communication:

Connect to fingerprint machine

Communication type: Ethernet

IP address: 192.168.1.201

Port: 4370

Communication key:

Machine Name: New Unit

Connection OK Cancel

If you don't set the password in device, you not require input password

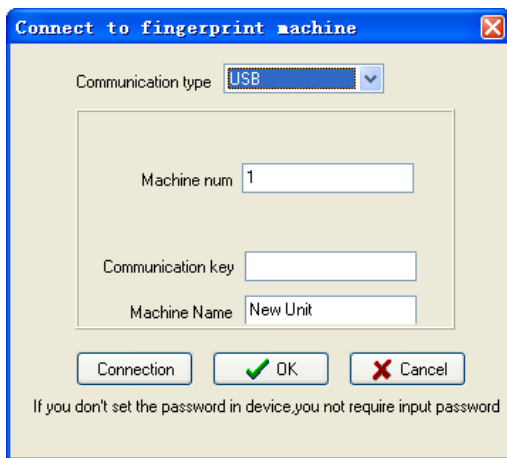
IP address: Default address is 192.168.1.201, please input the IP address of the FP Reader you want connect.

Port: The default port is 4370, it is needed to change.

Communication key and **Name** is the same configure as **RS232 /RS485**.

USB Communication:

This communication way need the device supports USB communication.



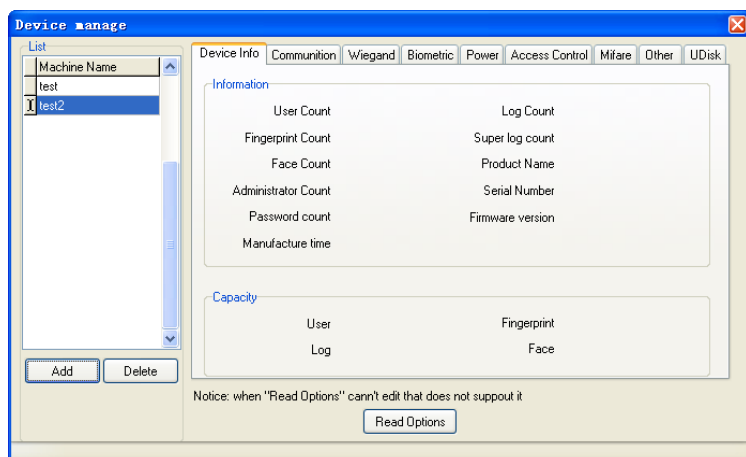
Machine num, **Communication key** and **Machine Name** is the same configure as **RS232 /RS485**.

After setup, click [**Test Connection**] button under window to test. If the system popup "**Successfully Connect**", click [**OK**] button to save the connecting parameters of this FP Reader. If the system popup "**Fail Connect**" dialog, please check the parameters and try again. Add the next fingerprint reader as this procedure.

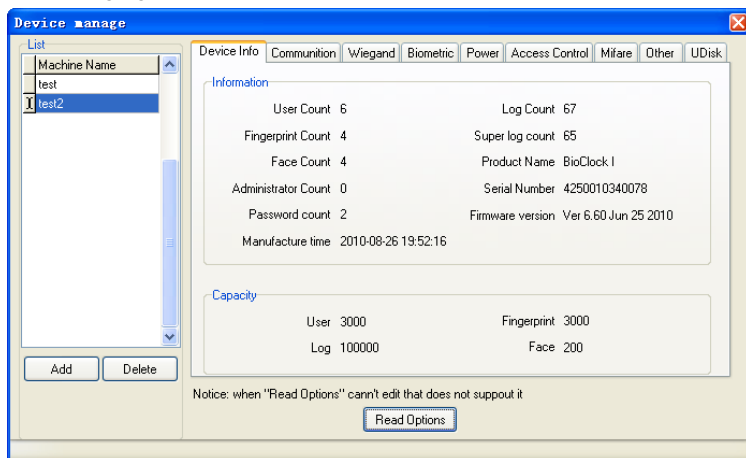
If you want delete a FP reader, select this unit, and click [**Delete**] button on underside.

4.1 Device Information

Click [**Device info**] in the [**Device manage**] item, display interface is following.



Click **[Read Options]**, the basic information of FP Reader will be listed, as the following figure.



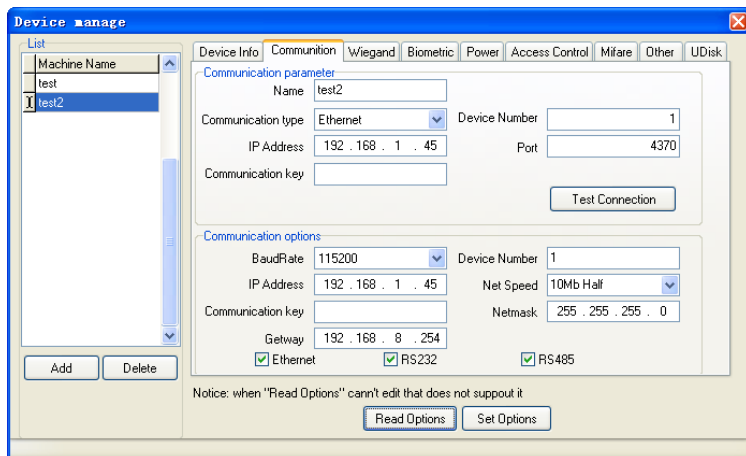
4.2 Communication


Communication Setting: Click **[Read Options]**, it shows the communication information of the current connecting device. Like as below

figure.

Communication Parameter: All kinds of communication parameter which is used for the connection of the software and the reader.

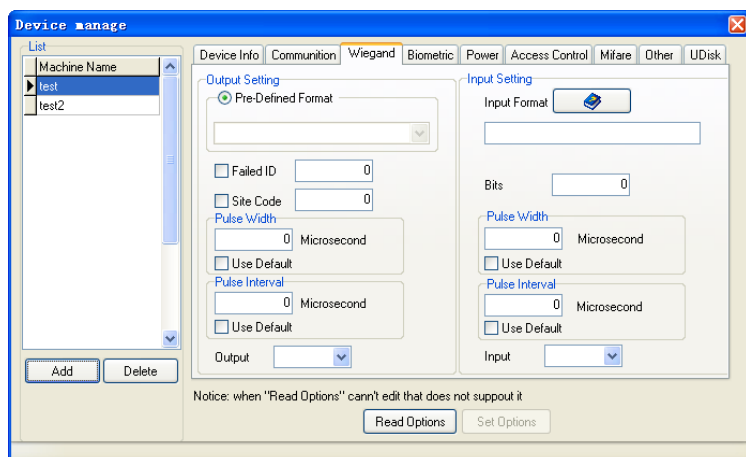
Communication Options: The Option of FP reader communication. If you want to change the communication configure, first click [**Read Options**] to obtain all origin parameters, then modify it as needed, and then click [**Set Options**] button, the modification will take effect after you restart the device.



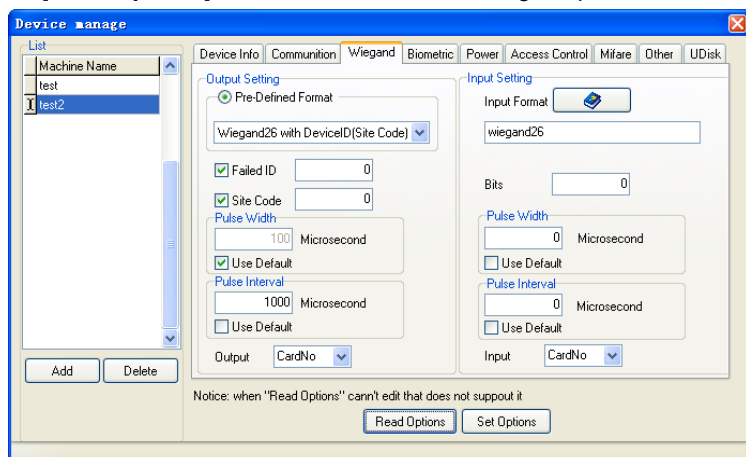
 **Note:** If you use RS232 to communicate, recommend to adopting 115200 Baud Rate, if you use RS485 to communicate, better to utilize 38400 Baud Rate.

4.3 Wiegand

Click [**Wiegand**] in the [**Device Manage**], display interface as following.



Click **[Read Options]** can obtain all the device wiegand parameters .



Wiegand Setting include Wiegand **output** and **input** setting.

Defined Format: These formats have been defined and built in the system, it needn't user to define the length of Bit and the location of information. There are four default defined formats: wiegand26 with device ID, wiegand34 with device ID, wiegand26 without device ID, wiegand34

without device ID.

The wiegand 26 with device ID means that the wiegand26 output format along with device ID number.

The wiegand26 without device ID means that the wiegand26 output format doesn't own the device ID.

Device ID is defined by following: If there is no set of the site code, then it will output machine code. And if the site code has been set, it will output the defined site code (which is similar to the machine code, they are different that this code is defined by user and can be used repeatedly, range is 0-255).

Fail ID: Export Fail ID after verification failed, no export when it has not been selected. Its output range is 0-65534.

Site Code: Similar to the machine code, the difference is that this code is defined by user and can be used repeatedly in different unit, range is 0-255.

Input format: Assigns Wiegand inputs format, following detailed introduction.

OEM code: Needn't to be defined for 26 bit-wiegand generally, find it from 37, 34 bit-Wiegand

Facility code: Machine number or refers to site code

ID Number: User serial number.

Use its first letter for respectively indicate (no matter it is in capital letter or small letter) in the format. ofOFI, the small letter express odd (odd), the capital letter refers to even (Even), Oo refers to OEM code, Ff refers to Facility code, li is ID number, P express the parity bit. The following is a demonstration with a standard 26bit-Wiegand input: PFFFFFFFFIIIIIIIIIIIIIP, Facility code and ID Number are both 1:

E	Facility code	ID Number	O
---	---------------	-----------	---

P	F	F	F	F	F	F	F	F	I	I	I	I	I	I	I	I	I	I	I	I	I	P	
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Total Bit: The length of output format.

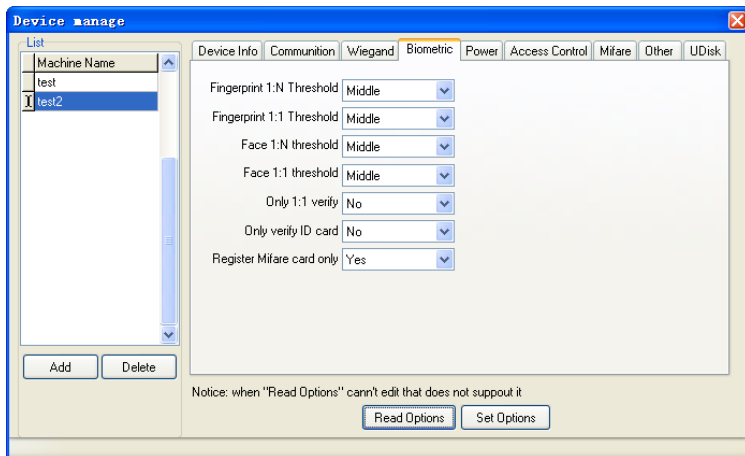
Pulse Width Time: The default to send pulse width time is 100μs, if the controller isn't able to receive the wiegand signal, can adjust value from 20 to 800.

Pulse Interval Time: The default value is 900 μs, can adjust from 200 to 20000.

Input/Output contents: ID or CardNo.

4.4 Verification

Click **[Biometric]** in the **[Device manage]** item. Click **[Read Options]**, following interface display.



Fingerprint 1: N Threshold: The default value is “Middle”, you can modify it properly.

Fingerprint 1:1 Threshold: It means the fingerprint verification threshold after presenting the card, the default value is “Middle”.

Face 1: N threshold: The default value is “Middle”, you can modify it properly.

Face 1:1 threshold: It means the user face verification threshold after presenting the card, the default value is “Middle”.

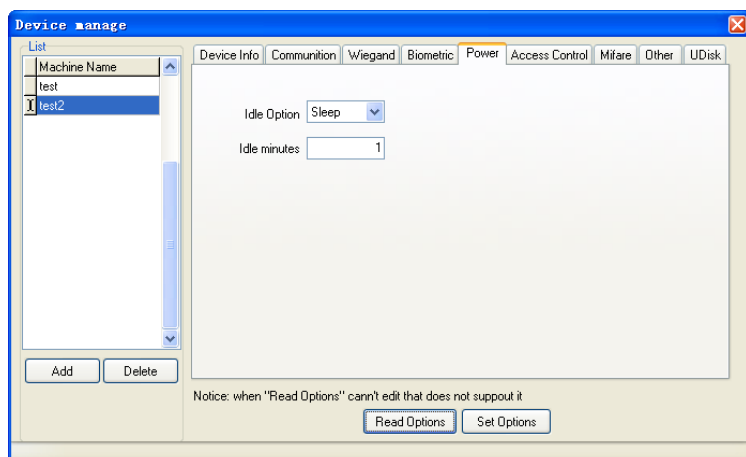
Only 1:1 Match: This feature is only available that a user own fingerprint, ID card or Mifare card for verification, if you choose [Yes] to this setup, must first present a card, and then press fingerprint. If doesn't slide a card, there is no reflect to fingerprint in the device.

Only Verify ID Card: It is mainly designed for ID card. When you choose [Yes], a user use ID card to verify directly, and needn't to press fingerprint. When you choose it as [NO], you must verify fingerprint after present the card.

Must Register Mifare Card: There are two statuses to register a Mifare card, if the card was configured to [Must Register], it is only to verify the user who's ID has stored in the FP Reader. The user without ID number will not be verified. When you choose the item as [NO], whether there is user's ID information in the device or not, it will export after the user and fingerprint template is verified successfully.

4.5 Power Management

Click [Power] button, and then click [Read Options] button, display the following interface.



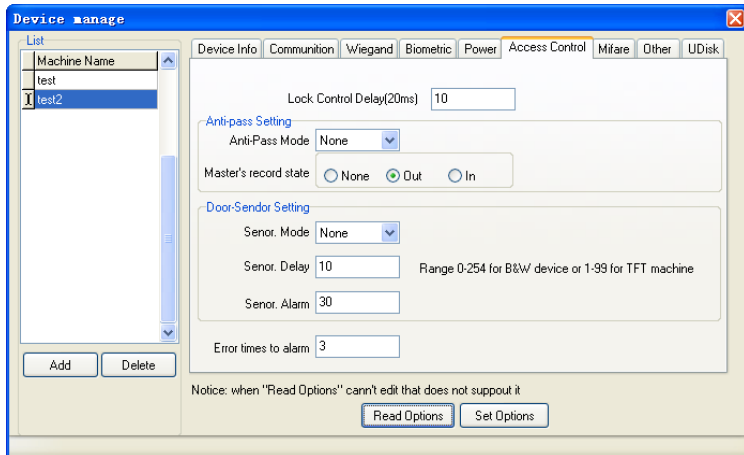
Firstly read the parameter of [Power], modify the state of [Idle Setup] and minutes of [Idle Time], then click the [Set Options] and restart the device to complete setting.

When the idle time is 0, then the idle setup function is off. When the value more than 0, the machine will enter into idle state after arrives at define time. You can resume normal working state via press the button on the device.

4.6 Access Control

Click **[Access Control]** button, and then click **[Read Options]**, display the interface as follow:

4. Device Management



Lock Control Delay: Apply to determine unlock hour, the minimum measured unit is 20 ms, in the normal condition that is 100-200 ms.

Anti-Pass Mode: Can be set to "None", "Out", "In", "InOut".

Master's record state: Can be set to "None", "Out", "In".

Sensor Mode: Set Door Sensor Mode. It can be set to "None", "NOpen", "NClose" state.

Sensor Delay: Set the sensor delay time when the door is opened. The sensor detect the door state only after this defined time. If the door state is not consistent with this parameter, the alarm will be triggered. Black and white screen device range is 0-254. Color screen device range is 0-99.

Sensor Alarm: Set the alarm time delay after the alarm is triggered. Range is 0-999 seconds.

Error times to alarm: Define the maximum error times to trigger alarm. When the verify is not through, and exceed this defined times, the alarm signal will be triggered automatically.

4.7 Mifare

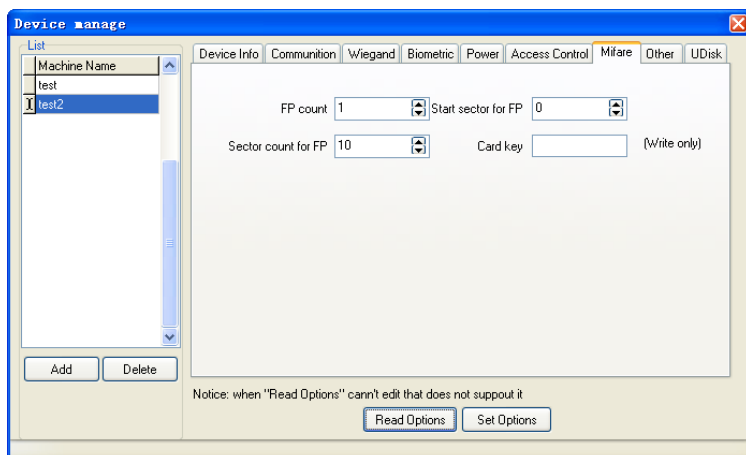
Click **[Read Options]** in **[Mifare]** menu, display as following.

FP Count: How many fingerprints stored in the Mifare card.

Start sector for FP: The first sector of Mifare card to store fingerprint.

Sector count for FP: Fingerprint appropriate total sector.

Card key: Read and write password of card, you can only setup, can't read it.



4.8 Other Setup

Click **[Other Setup]**, and then click **[Read Options]**, the following interface appear.

Restart Device: Click the button to restart FP Reader.

Power off Device:

Update firmware: **Notice:** Please do not upgrade the firmware at your discretion because it may bring problems and affect the normal use of the device. Contact our distributors for technical support or upgrade notification.

Clear admin privilege: This function can clear all administrator privilege which has registered in the reader.

Initial Device: This function is mainly used to clear all data in the FP Reader.

Sync time: Set the device time same to the PC time.

Capture Fingerprint: This function can be used to view fingerprint image. If you want to check the fingerprint image, please place finger on the sensor window, and then click the button, and will see the fingerprint image.

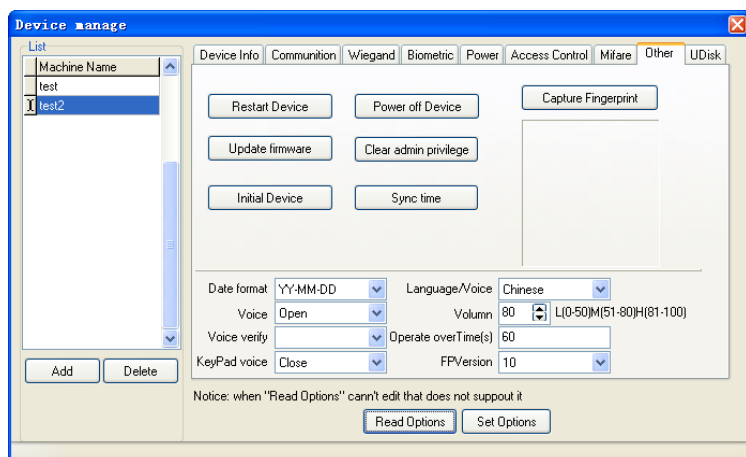
Date format: Select the date format in the down drop menu, this date format is the date display format on the device starting interface.

Voice function: Including voice, voice verifies, keypad voice, you can choose to open or close. You can set the voice volume too. This function is available in the FP Reader which supports voice hint function.

Operate over time(s): Set the device operation timeout.

Operate overtime: Set the device operation overtime, 30s by default.

FPVersion: Select the fingerprint algorithm version, 9.0 or 10.0. These two version are not compatible, please choose carefully.



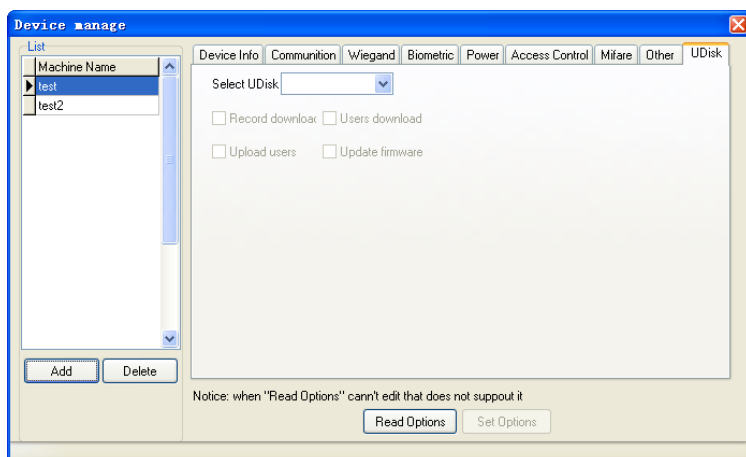
4.9 U disk Setting

You can use the Access Management software to set the U disk configuration file. When the device is connected with U disk, it can execute operations such as Record download, User download, Upload users and Update firmware.

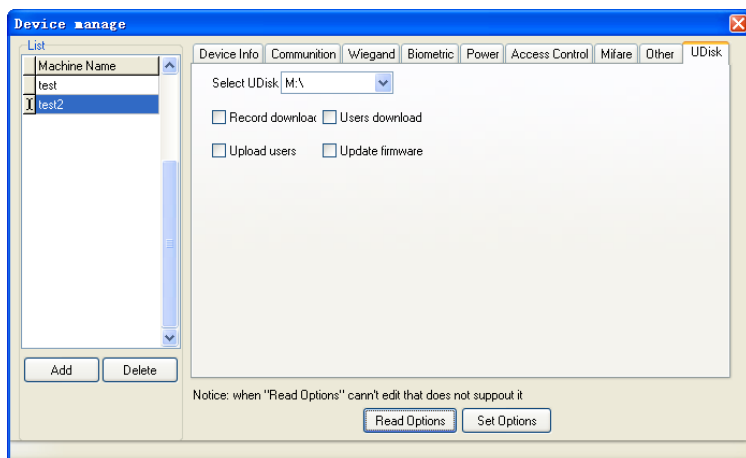
Using PC software to create and modify configuration files steps:

1. Click [U disk] in [Device manage] menu, enter the following interface.

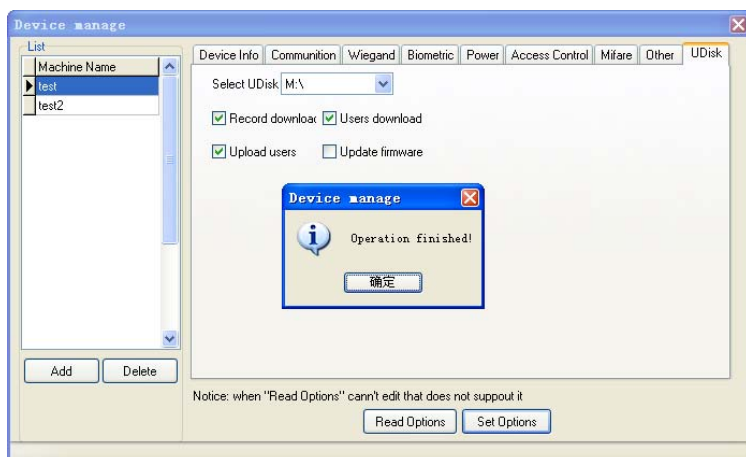
4. Device Management



2. Select U disk from the down drop menu, click the [Read Options], the interface display Record download, User download, User upload and Update firmware four options.



3. Select the need for the operation, click [Set Options] button, the system prompts "Operation finished", as shown below.



Open the U disk you can see the configuration file named `operatemode.cfg`.

The operation to execute the U disk configuration file please refer to the related device user manual.

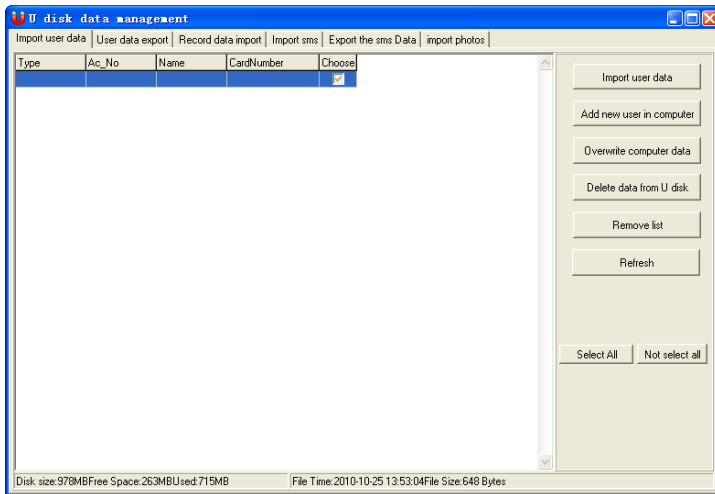
5. U Disk Management

In general, you can use RS232, RS485, TCP/IP or USB to exchange the attendance records with device.

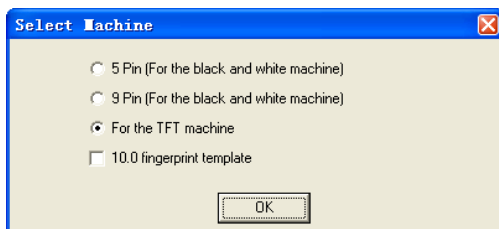
If the communication method above are not available, you can use U disk to download or upload the user information and fingerprint, or download the attendance records.

5.1 Import User Data

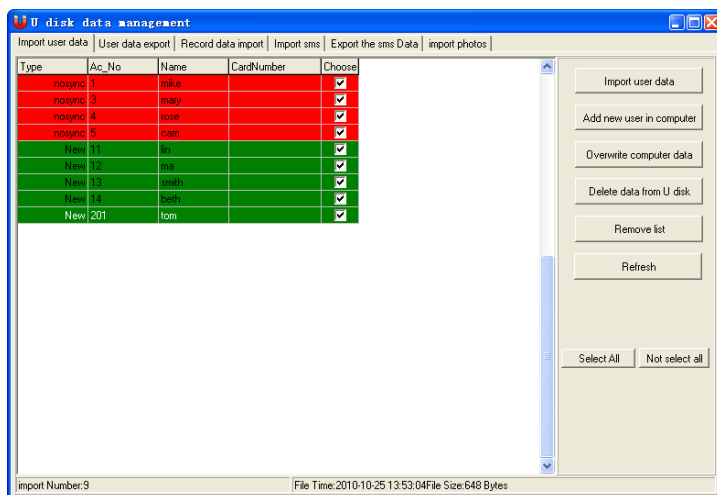
1. Plug the U disk into the PC USB slot. Click **U Disk Management** in the **Base Options**, and enter the U disk management interface. Like as follow figure.



2. Click **Import User Data** button. The system will prompt **Select Machine** dialog. The imported user data format is different according to the machine type, so you need select the type first.



3. After that, click **OK** button, the system will automatically search the user data and load it into the system from the U disk. If a new use is found, the data will shown in green color. In the list the records with red color show this record do not synchronization with data of software.



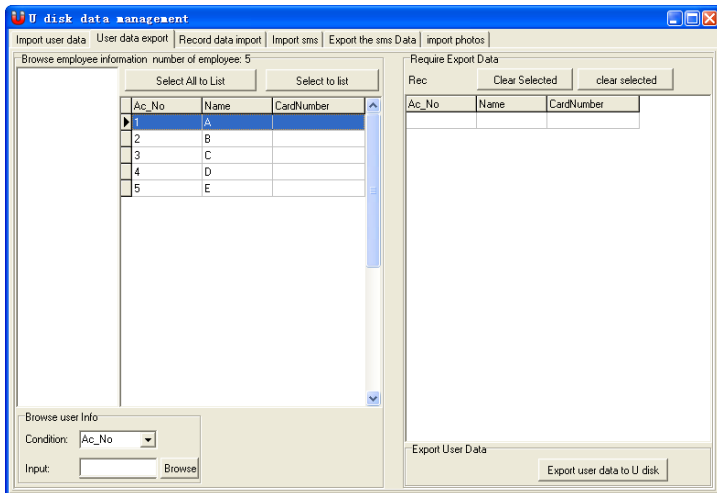
- **Add new user in computer:** Import the new user in buffer area to the computer.
- **Overwrite computer data:** Import the selected user in buffer area to the computer.
- **Delete data from U disk:** Delete user data from U disk.
- **Remove list:** Clear the user list in buffer area.

- **Refresh:** Refresh the user data in buffer area.

5.2 User Data Export

Through U disk Management interface, you can export the user data to U disk, and then upload the data to the device.

Plug the U disk into the PC USB slot. Click **U Disk Management** in the **Base Options**, and enter the U disk management interface. Select **User data export** option, like as follow figure.



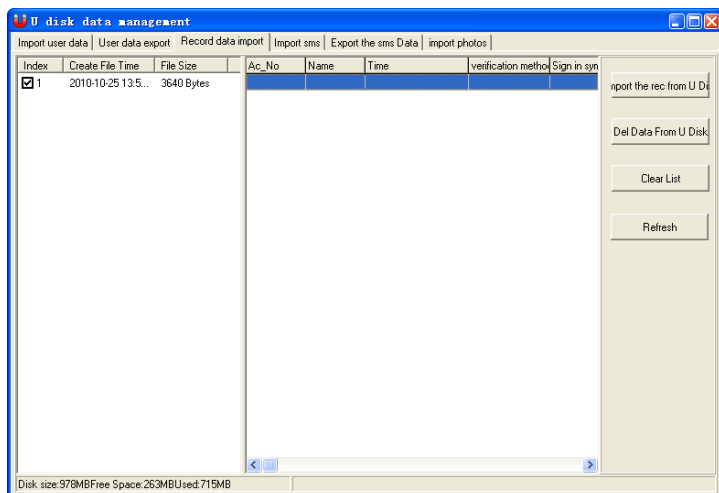
Double click staff record or selected staff and click **Select to list** add an employee information to the right side. If there are a lot of staff record, ability to show all staff information to be queried through staff information query function. The query condition such as Ac_No, Name, CardNumber is available.

Click **Export user data to U disk**. Then all records shown in the buffer area exporting to U disk.

5.3 Record Data Import

Through U disk Management interface, you can export the record data to U disk, and then import the data to the system.

Click **U Disk Management** in the **Base Options**, and enter the U disk management interface. Select **Record data import** option, like as follow figure.



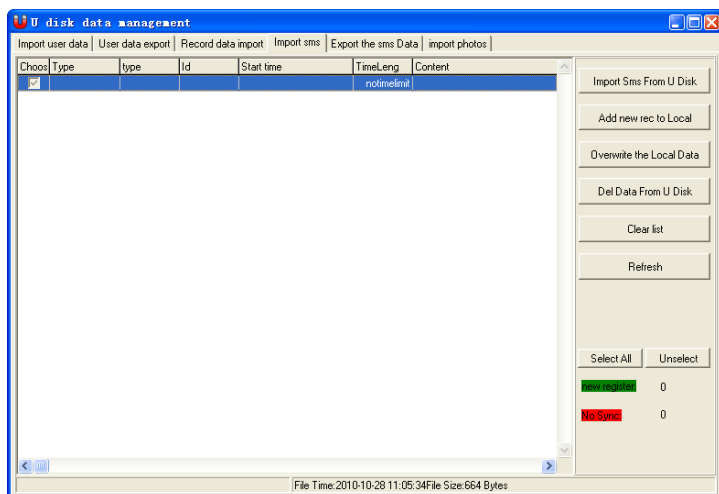
Click **Import the record from U disk**, then the system importing the data. When its finished, all records shown in the buffer area.

- **Delete data from U disk:** Delete record data from U disk.
- **Clear list:** Clear the record list in buffer area.
- **Refresh:** Refresh the record data in buffer area.

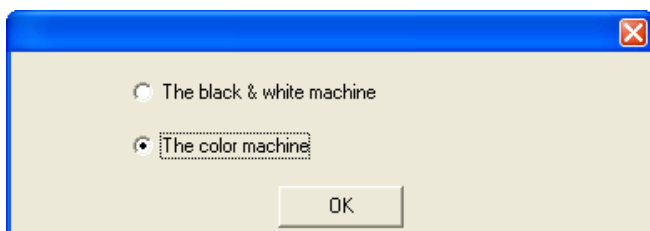
5.4 Import Sms

Plug the U disk into the PC USB slot. Click **U Disk Management** in the **Base Options**, and enter the U disk management interface. Select **Import Sms** option, like as follow figure.

5. U Disk Management



Click **Import Sms from U Disk** button. The system will prompt **Select Machine** dialog, the import sms data format is different according to the machine type, so you need select the type first.



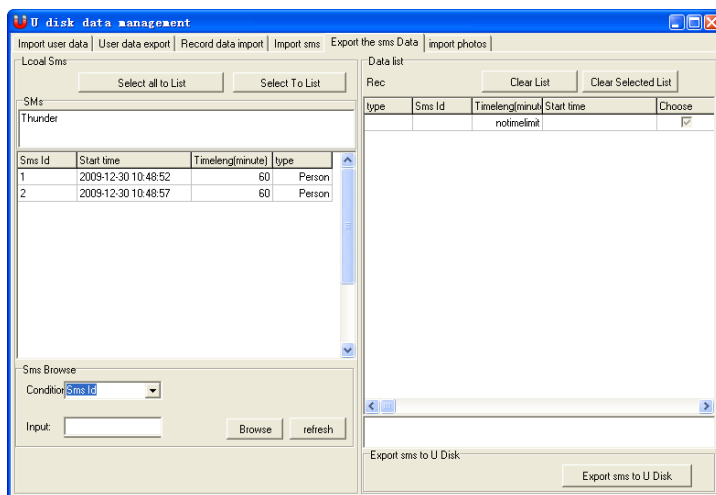
Click **OK** button, the system will automatically search the sms data and load it into the system from the U disk. After that, the system will prompt the number of import sms, and shown them in list.

- **Add new record to local:** Import the new sms in buffer area to the computer.
- **Overwrite the local data:** Import the selected sms in buffer area to the computer.

- **Delete data from U disk:** Delete sms data from U disk.
- **Clear list:** Clear the sms list in buffer area.
- **Refresh:** Refresh the sms data in buffer area.

5.5 Export the Sms Data

You can export the sms data to U disk, or import the data to the other device through U disk. You can select the desire sms to upload.



The local sms area will show all the sms in software. When you select a sms, the content will show at the sms dialog. If there are a lot of staff record, ability to show all sms information to be queried through staff information query function. The query condition such as Sms Id, content, public, person is available.

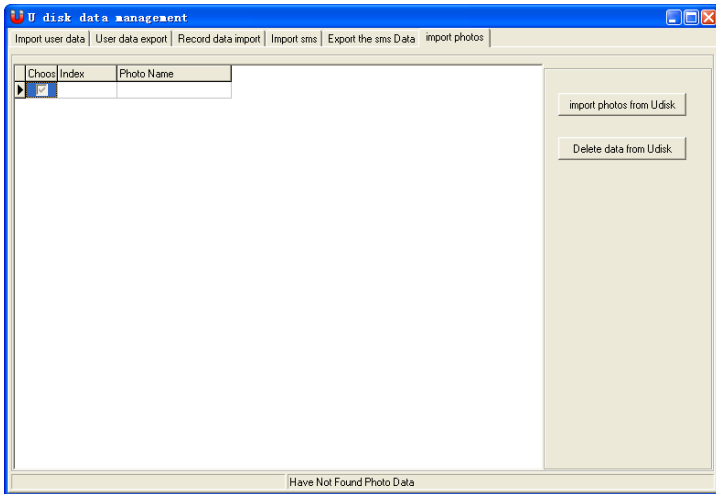
- **Select all to list:** Select all the sms data to data list.
- **Select to list:** Select the sms and click **Select to list**, the selected sms data shown in data list.
- **Clear list:** Clear the sms list in data list.

- **Clear selected list:** Remove the selected list in data list.

Click **Export sms to U disk**. Then all records shown in the data list exporting to U disk.

5.6 Import Photos

Plug the U disk into the PC USB slot. Click **U Disk Management** in the **Base Options**, and enter the U disk management interface. Select **Import photos** option, like as follow figure.



Click **Import photos from U disk**, then the system importing the user photos. When its finished, all photos shown in the buffer area.

- **Delete data from U disk:** Delete photo data from U disk.



Note: U disk function require the device support.

6. SMS Management

In some models of device, we offer the function to send scheduled SMS to the user or public. We just need to set the SMS in the software, and then upload to the device. The public SMS will appear at the device for all the user to view, and will appear always. The user SMS will show after user verification. So as to reduce the staff workload and improve the work efficiency.

6.1 SMS Content Manage

Enter the SMS Management interface:

Click **SMS Management** in the **Base Options**, like as follow figure.

SMS MANAGE

SMS CONTENT MANAGE | Employee SMS customization inquiry

Select All | Unselect

Sms: Thunder

Smsid	Start time	Timeleng(Minute)	Type
1	2009-12-30 10:48:52	60	User
2	2009-12-30 10:48:57	60	User

Send SMS | Employee SMS customization

Delete: ☒ SMS of attendance machine ☐ User customizes message

Execute

COMMU SETTING

commu type: Rs232/Rs485 | SAVE

Machinenum: 1

Port: COM1

baudrate: 115200

Password: | Connect Test

Browse

Condition: Smsid

input: | browse

Sms Info

ADD | EDIT

DELETE | REFRESH

Sms Number: 2

1. Communication Setting

There are two ways for device communication. Similar to the device connection in [4. Device Management](#). After complete setup, click [Test

Connection] button to test, if it is succeed, the system popup “Successfully Connect” dialog, and the button turn to [Disconnect]. If it is fail, the system popup “Fail Connect” dialog.

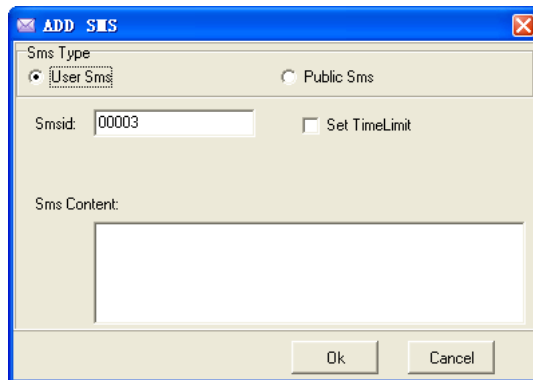
2. SMS Query

The system support to query SMS by Smsid, Sms Content, Public Sms, User Sms, etc. Click [Condition] down-drop menu, select the condition and input the information, then you can view the query result in the sms list table by click [browse] button.

3. SMS Management

The system support to manage the SMS information, such as ADD, EDIT, DELETE and REFRIESH functions.

ADD: Add a new SMS. Click [ADD], the following interface appear:

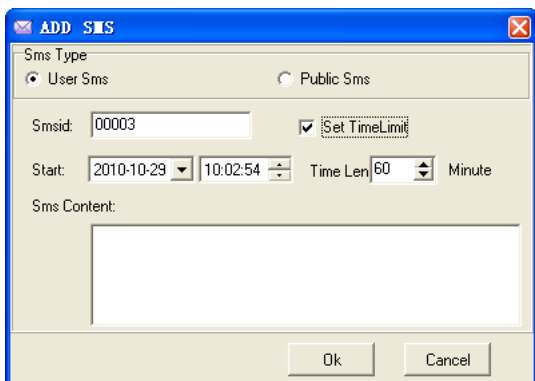


Public SMS: Indicate the SMS for the public to view. The SMS will show after the device start, and appear always.

User SMS: Indicate the SMS for the user to view, it will appear after user verification.

Set TimeLimit: Click this item, another line will show in the interface, as following figure. You can define the start time and time length of the SMS

valid time.



DELETE: Select a SMS, and click [DELETE] button, the system will prompt “Are you sure to delete selected short message?”, click [OK] and another prompt will show: “Whether delete all short messages in attendance machine at the same time”, click [OK] to confirm deletion.

EDIT: Select a SMS, and click [EDIT] button, to modify the SMS information, such as SMSid, valid time and SMS contents.

REFRESH: After SMS query, the SMS list will show all the query result, click [REFRESH] to return to the whole SMS list.

4. Send SMS

Select the SMS in the left SMS list, and click [Send SMS] button to send the SMS.

6.2 Employee SMS customization

Click [Employee SMS customization], the following interface appear:

6. SMS Management

Employee SMS customization

Browse

condition: **Department** Input: Browse Refresh

User Info

Select All UnSelect All

Department	A/C-No	Name	Choos
Factory	3	C	<input type="checkbox"/>
Factory	4	D	<input type="checkbox"/>
HR	5	E	<input type="checkbox"/>
R&D Dept.	1	A	<input type="checkbox"/>
R&D Dept.	2	B	<input type="checkbox"/>

SMS

Smsid	Start time	Timeleng(Minute)	Choos
1	2009-12-30 10:48:52	60	<input type="checkbox"/>
2	2009-12-30 10:48:57	60	<input type="checkbox"/>

Summer coming

Oper Select

☒ Send immediately ☐ Not send temporarily

Ok cancel

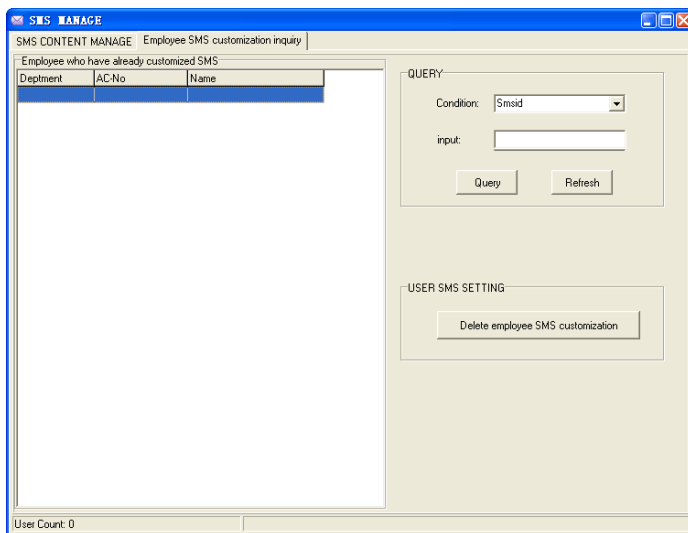
User Count: 5 Sms Number: 2

User Info: To list all the employee in the system, you can select multi user to send the customized SMS.

SMS: To list all the SMS added in the system.

Oper Select: If the software have connected with the device, you can select [Send immediately], otherwise, you can select [Not sent temporarily], and return to the SMS management interface. Select the SMS you want to send, click [Send SMS] to send the SMS. Or send the SMS through U-disk. For the detail please refer to [5.5 Export the SMS data](#).

Click [Employee SMS customization inquiry] and enter the query interface.



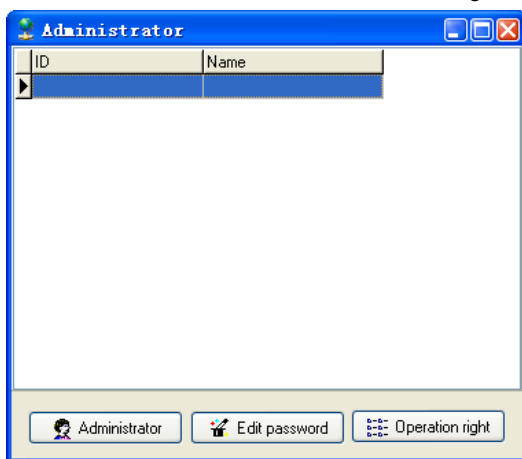
You can select the query condition from the drop-down menu: query by SMS id, Department, Attendance ID and name. If you don't need the SMS, you can also delete the SMS by click the [Delete employee SMS customization] button.

7. System Management

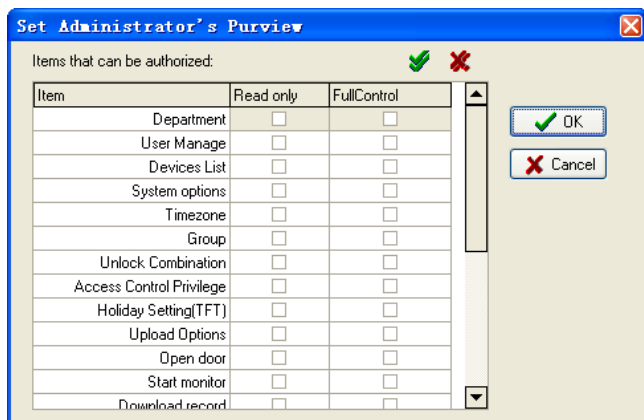
System Management includes Operator Management, System Operation Log, Backup Database, Clear Obsolete Data, Initial System, Set Password of Database and System Options.

7.1 Operator Management

Click [**Operator Management**] in the [**System Manage**] menu, Popup the main interface of administers maintained, like as following



Click [**Administrator**], Popup the three item of [**Add department Administrator**], [**Add Administrator**] and [**Delete Administrator**]. Click [**Add Administrator**], and then popup a user list frame, select a user to be adding as an administrator, and the click [**OK**] to popup a distributing privilege list, as following figure.



Put a remark in the administrator privilege, and then click **[OK]**.

If want to cancel administrator, select the Administrator firstly, and then click **[Delete Administrator]** to complete the operation process.

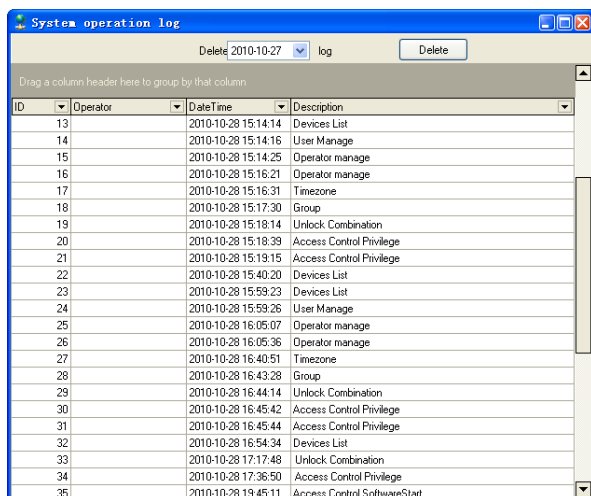
The operation of **[Add department Administrator]** is same to **[Add Administrator]**.

It is able to modify administrator password and operation privilege after an administrator is added.

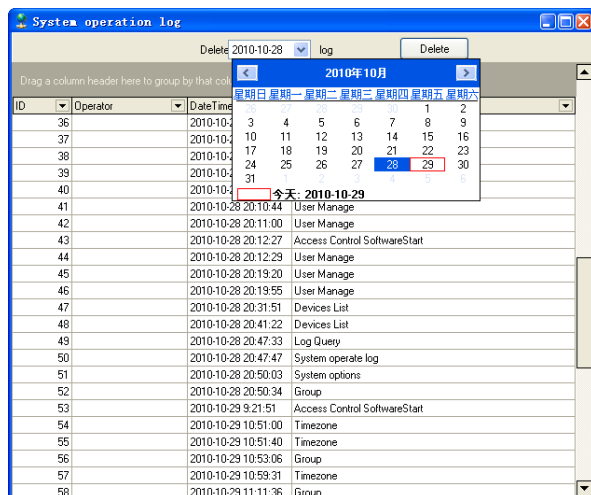
7.2 System Operation Log

The system operation Log is a track record which records this software operation history, and utilize list mode to record all operation.

7. System Management



Click [Delete], this operation is available to delete operation log to the defined previous date, appear following figure.



7.3 Data Maintenance

The Data maintenance is, consist up Backup Database, Compact the Database, Clear Obsolete Data, three module build up.

1. Backup Database

Click **[Backup Database]** in the **[System Manage]** menu, popup a dialog-box to backup database, you can name it as your favor, and save it in the defined location.


2. Compact the Database

Click **[Compact the Database]** in the **[Data Maintenance]** menu, to compact the database, it is only capable to Access Database.

3. Clear Obsolete Data

You can use this function to clear old data which are useless to utility, click **[Clear Obsolete Data]** in the **[Data Maintenance]**.

Click the down drop menu to choose the date, and select the old record backup directory, then click **[OK]** button to clear old data.

 **Notice:** The delete content doesn't include the ending date be selected.

7.4 Initialize System

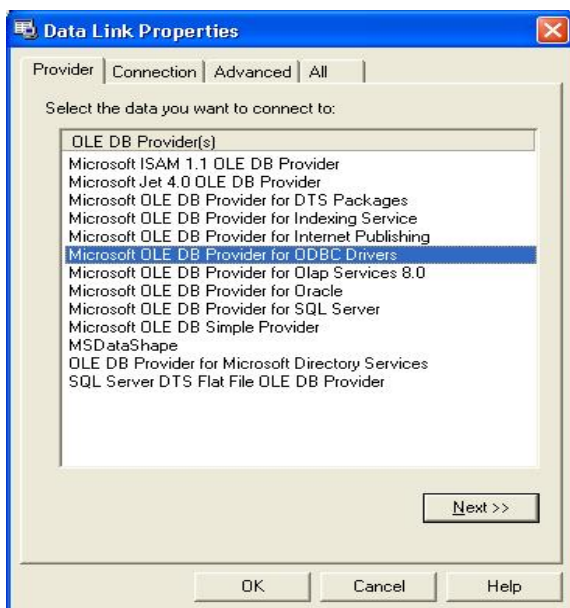
Click **[System Init]** in the **[System Manage]** menu, popup a warn dialogs box, like as following figure, executes the command all the system will be initialized, after this operation all data will be cleared.

 **Notice:** use this operation with caution.

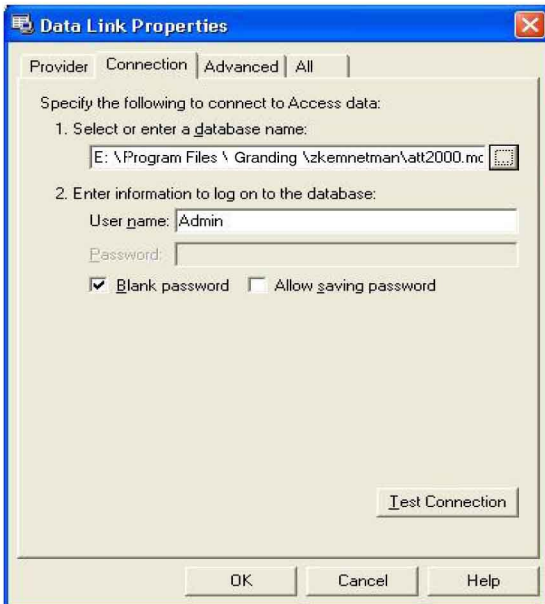
7.5 Set Database


1. Connecting Microsoft Access Database setup

(1) Provide program to select Microsoft Jet 4.0 OLE DB Provider;



(2) Click **[Next]** or **[Connect]** enter the following interface.

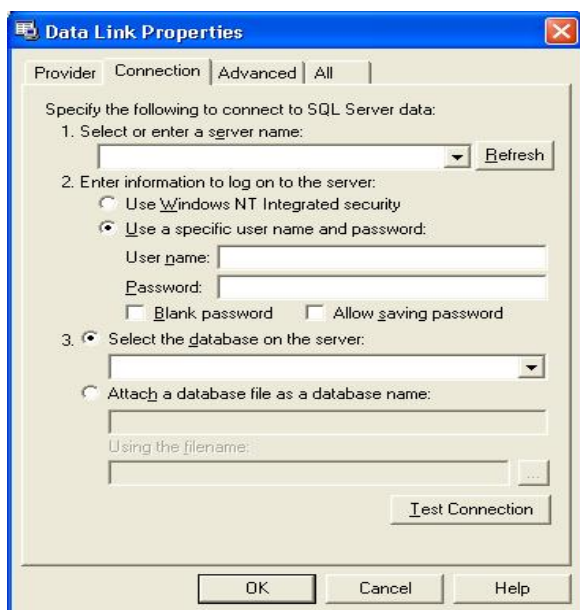


Click  button, Can select the database file, the default name is att200.mdb, according to real condition to renew setup of the database connection.

2. SQL Server Database Connecting Setup

First you should establish the empty database on the database server. You can find a script file with the name of sqlserver.sql in the directory of installing CD. The empty database is established in the front of the searcher of SQL Server, and then opens the sqlserver.sql script files, to run database which is to create this software.

In the Provider Select Microsoft OLE DB Provider for SQL Server, click [Next] or [Connect] to enter this following.



Confirm the server name for storing this database, information for logging on this server, and the database name. After running test connection successfully, click [OK] button to complete settings.

7.6 Set Password of Database

User who needs to encrypt this software database can utilize the function to encrypt the database. We strongly suggest that users who use an Access database encrypt the database in order to ensure security. Please distinctly keep in mind the password after setting it.

7.7 System Options

Open [System Options] in the [Base Options], the following interface appears.

System setup

Automatic monitoring settings

Automatically monitor

☐ When program starts, activate automatic monitor

Default device polling cycle (second)

Keep the number of device (Range 30000-120000)

Times of reconnection due to failure (Range 3-10)

Activate monitor in time zone

Download log time

Sync time

☒ The system will use default privilege while it don't assign privilege for user.

☒ After assigning privilege for user, along with uploading user the system upload User privilege.

☐ In downloading attendance records process, add the user when there is no local user

Anti-dismantle alarm

Unauthorized alarm

Duress alarm

Improperly closed door

Open the door by accident

company name

☒ Set database connection ☐ When start-up Windows, start-up this program

When program starts, activate automatic monitor

If this option is selected, program start will enable automatic poll all devices that has been connected with. If this option is not selected, program start will not enable poll.

Default device polling cycle (second)

During device continue poll, some fingerprint machines may disconnect temporarily due to various reasons. Here, you can modify device polling cycle in second (it is recommended to set to 120).

Keep the number of device

Device record number means user attendance records that are downloaded in every device. You can enter a record number. If actual

record number exceeds the pre-set value, the software will clear all fingerprint records stored in fingerprint machine. For example, record number to store is set to 30000, when record number downloaded is 30001, all fingerprint records in fingerprint machine will be deleted and record number downloaded resets to 0.

Times of reconnection due to failure:

Count for continuous failure retry (it is recommended to set to 3) that is convenience to reconnect automatically under the condition of fingerprint machine recovers normal connection.。

Activate monitor in time zone:

Here, we can define one time zone to run monitoring. If run uninterrupted polling, it will bring huge burthen to whole monitoring network. You can define one time zone to run monitoring, in order to reduce burthen of monitoring network. Please pay attention to time format, such as 06:00-22:00.

Download log time:

Set the cycle to download operation log automatically.

Sync time:

You can define a time to synchronize time of all fingerprint machines that have been added into device. Please pay attention to time format, such as 10:00

Set alarm sound:

Set all kinds of alarm sounds. Click [Set] button browse to select the desired audio file, and then click [Open] to complete setting.

The system will use default privilege while it don't assign privilege for user: Tick the box to confirm.

After assigning privilege for user, along with uploading user the system upload user privilege: Tick the box to confirm.

In downloading attendance records process, whether to add the user when there is no local user: Tick the box to confirm.

Company Name: The unit name is used in the software.

Set Database connection:

Click [**Set Database Connection**], will popup the window of the defined path database, please refer to [7.5 Set Database](#).

When start-up Windows, start-up this Program:

After select this item, when the PC start, the program will run automatically, otherwise, when the PC start, the program will not run automatically.

8. Access Control Setup

Access control setting is to set unlock time and assign privilege for registered users. Settings of each user consist of three time zone settings and one group setting. Relationship between time zones is “OR”. Group also consists of three time zone settings and by the same token, relationship between these three time zones is “OR”.

Simply put, if you want to keep a registered user in unlock status. Firstly the group that this user is in should be defined in unlock combination (one group can be defined in one combination together with other group, but these groups are required to unlock door together). Second, current unlock time is in any availability range of user time zone and time zone of its group.

Under system default, a new registered user is in Group 1 and group combination is Group 1. So new registered user is in unlock status by default. If a group that user is in is not defined in group unlock combination setting, then the user cannot unlock door.

8.1 Time Zone

1. Click [Time zone] from Drag-down menu of [Access Control Options], or click the [Time zone] shortcut in the main interface, window of adding Time zone will pop up.

AC Timezones option

Add Edit Delete

		Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
ID	Description	Start	End	Start	End	Start	End	Start	End	Start	End	Start	End	Start	End
1	first	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59

2. Click [Add] button and system will pop up a timetable from Sunday to Saturday. Here, you can define any time zone you may use.

Timezone option

select time zone ID: 1 Description: first

Sunday Monday Tuesday wednesday thursday Friday Satday

00:00 00:00 00:00 00:00 00:00 00:00 00:00

23:59 23:59 23:59 23:59 23:59 23:59 23:59

OK Cancel

3. Then click [OK] to save the time zone.

8. Access Control Setup

		Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
ID	Description	Start	End	Start	End	Start	End	Start	End	Start	End	Start	End	Start	End
1	first	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
2	afternoon	12:00	23:59	12:00	23:59	12:00	23:59	12:00	23:59	12:00	23:59	12:00	23:59	12:00	23:59

4. If you want to use several time zones, continue to click [Add]. The system support up to 50 time zone.

In addition, time zone can be edited and deleted.

8.2 Group

1. Entered the "Group" setting interface: Through bar options of the system menu: Access Control Options -> Group, or through shortcuts button options of the system: Group, Enter the group setting interface.

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
2		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
3		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

2. Group editing. Left click item that need to edit with cursor to enter the

editing state.

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
2		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
3		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

3. Through drop-down box to choose the time zone .

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		1	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
2		1	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
3		2	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

4. Through the drop-down box to choose verification ways.

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
2		0	0	0	01FP/PW/RF/FACE	<input type="checkbox"/>
3		0	0	0	1 FP	<input type="checkbox"/>
4		0	0	0	2 PIN	<input type="checkbox"/>
5		0	0	0	3 PW	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

5. If you want the time zone in group take effective on holiday, selected it by

cursor clicks, if you want the holidays is invalid, it can not selected.

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		0	0	0	FP/PW/RF/FACE	<input checked="" type="checkbox"/>
2		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
3		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

6. Set up is completed, click on "Save" to save.

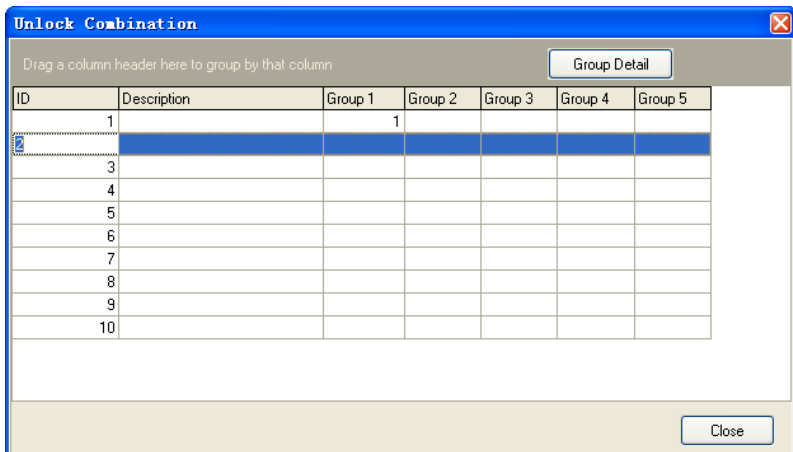
8.3 Unlock Combination

1. Entered the "Unlock Combination" setting interface: Through bar options of the system menu: Access Control Options-> Unlock Combination, or through shortcuts button options of the system: Unlock Comb, Enter the Unlock Combination setting interface.

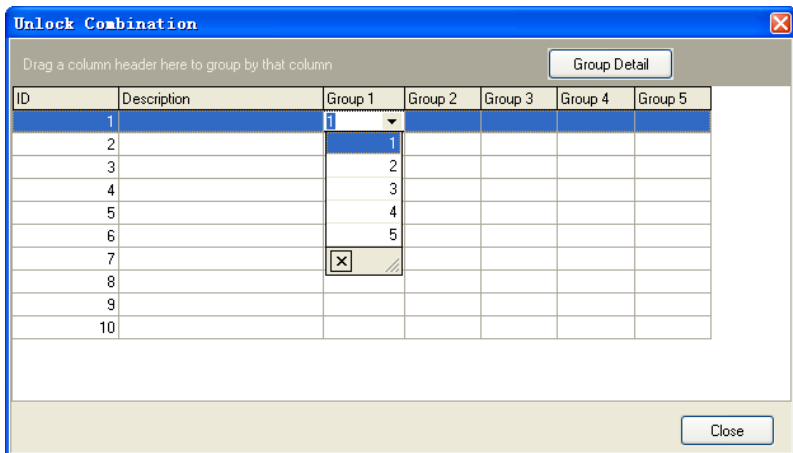
ID	Description	Group 1	Group 2	Group 3	Group 4	Group 5
1		1				
2						
3						
4						
5						
6						
7						
8						
9						
10						

2. Unlock Combination editing. Left click item that need to edit with cursor

to enter the editing state.



3. Through drop-down box to choose the group number



4. If you forgot the group definition, click Group Detail to see the exist group, and return to step 3 to select group.

8. Access Control Setup

Group	Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1			2	0	0	FP	<input checked="" type="checkbox"/>
2			0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
3			0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4			0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5			0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

Close

5. Set others unlock combination as step 3-4. After setting up click "Close" to save and quit.

8.4 Access Control Privileges

1. Entered the "Access Control Privilege" setting: Through the system menu bar options: Access Control Settings -> Access Control Privilege, or through directly shortcuts button of the system : Access Control Privilege, enter Access Control Privilege interface.

Ac Privilege option

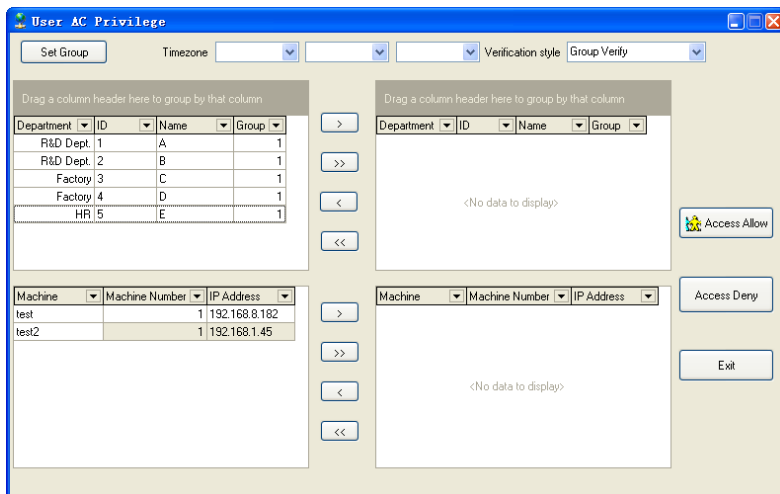
Edit Privilege

Drag a column header here to group by that column

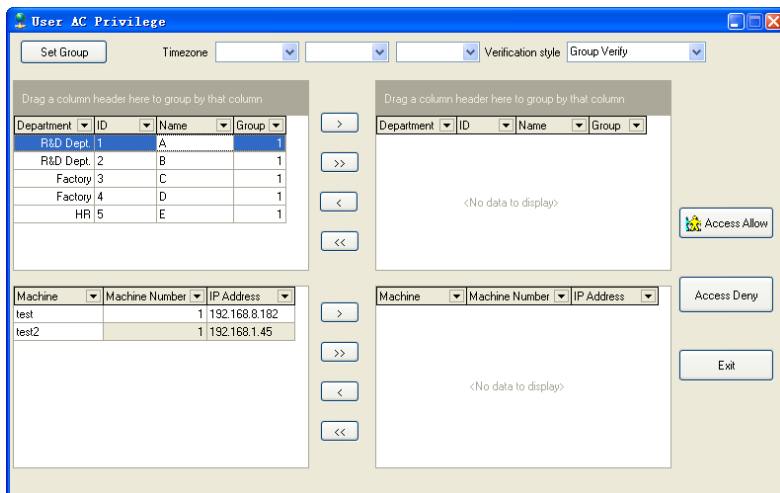
ID	Name	Group	Is Use Group	Timezone 1	Timezone 2	Timezone 3	Door(AC machine)	Verification style
<No data to display>								

2. Click on "Edit Privilege" button and enter the Access Control Privilege to

edit the interface, shown such following.



3. Default users belong to Group 1, if need be assigned to other user groups, the need for users to re-allocation group. Here we illustrate: No. 1 users assigned to Group 1. First selected No. 1 users, shown as following.



8. Access Control Setup

4. Click on the "Set Group" button and enter "the group setting" interface, select group 2.

Group	Description	Timezone1	Timezone2	Timezone3	Verification style	Holiday take effect
1		2	0	0	FP	<input checked="" type="checkbox"/>
2		1	0	0	RF	<input type="checkbox"/>
3		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
4		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>
5		0	0	0	FP/PW/RF/FACE	<input type="checkbox"/>

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

OK

5. Through the above steps, the users will be assigned to the second group, shown as following.

Set Group Timezone Verification style Group Verify

Drag a column header here to group by that column

Department	ID	Name	Group
R&D Dept.	1	A	2
R&D Dept.	2	B	1
Factory	3	C	1
Factory	4	D	1
HR	5	E	1

> >> < <<

Drag a column header here to group by that column

Department	ID	Name	Group
<No data to display>			

Access Allow

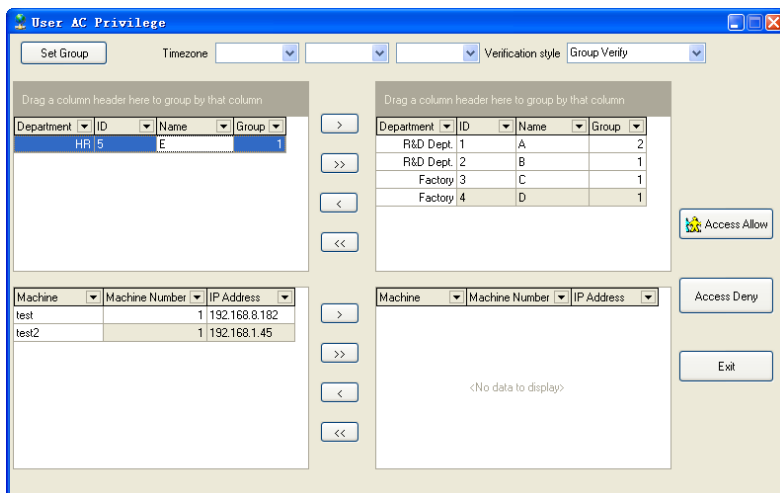
Machine	Machine Number	IP Address
test	1	192.168.8.182
test2	1	192.168.1.45

> >> < <<

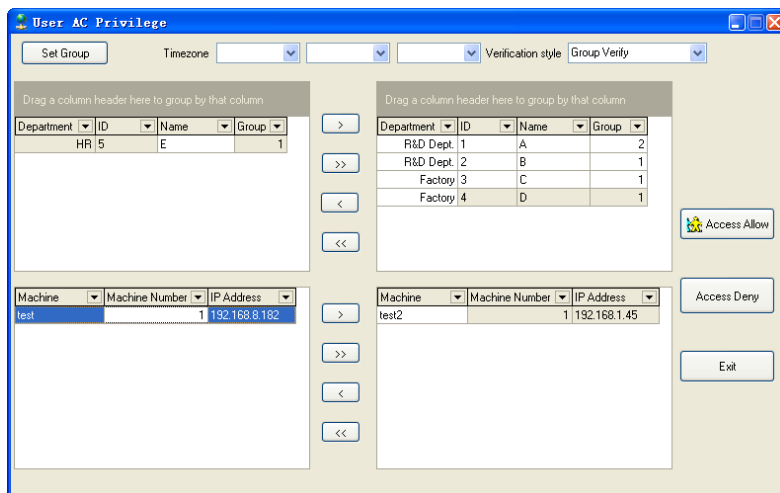
Access Deny

Exit

6. Follow the 3-5 steps, set up the group those users respective. After the setting completed, through ">/>>" button, a single or all of users will be moved to the right critical areas, waiting for the Privilege setting. Shown as following.

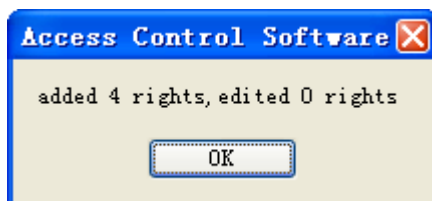


7. In the device list choose the device that need to upload Privilege. Through ">/>>" button, single or all of the device will be moved to the right the critical region, waiting for Privilege setting. Like following interface.

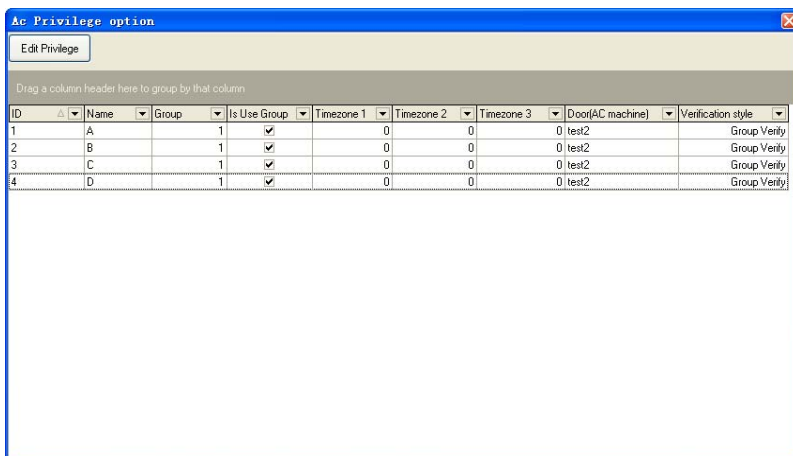


8. After users and device is selected, click on "Access Allows" button, the

group Time zone which is used by user in the critical periods will be assigned to the selected devices. After distribution is successful, prompt will appear shown as following

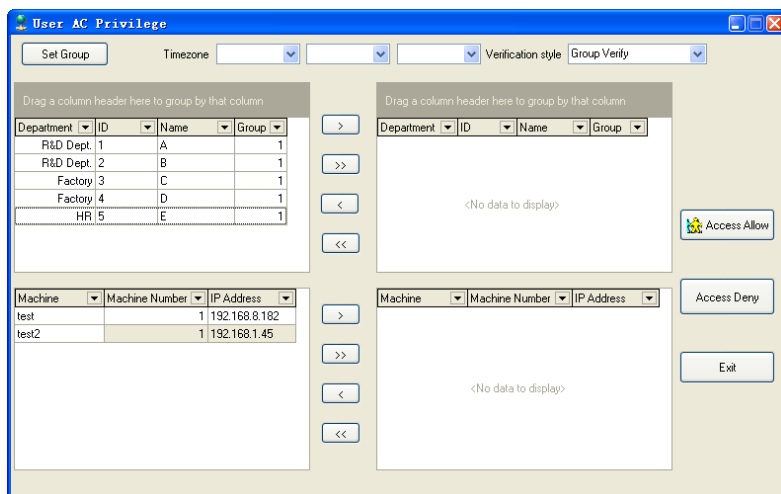


9. In the "User Access Control Privilege" interface, click "exit" button and enter the "Access Control Privilege Setting" and synchronize set up information of user groups will display in the list. Shown as following.



Set up the user doesn't use the Access Control Privilege of group time zone:

1. If a user do not use group time zone when she/he belong to a group, please enter the "User Access Control Privilege" setting interface.



2 Select a user and the applied device, click [Access Deny] button, pop up the following interface.



3. After completing, in the "user Access Control Privilege" interface, click "exit" button and enter the "Access Control Privilege Setting" and synchronize set information of user groups will display in the list. shown as following.

8. Access Control Setup

Ac Privilege option

Edit Privilege

Drag a column header here to group by that column

ID	Name	Group	Is Use Group	Timezone 1	Timezone 2	Timezone 3	Door(AC machine)	Verification style
1	A	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify
2	B	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify
3	C	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify

4. Click [Edit Privilege], select the user, the device, the using time zone and the verification style, and click [Access Allow] button.



5. After modification, a new record list in the following interface.

Ac Privilege option

Edit Privilege

Drag a column header here to group by that column

ID	Name	Group	Is Use Group	Timezone 1	Timezone 2	Timezone 3	Door(AC machine)	Verification style
1	A	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify
2	B	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify
3	C	1	<input checked="" type="checkbox"/>	0	0	0	test2	Group Verify
4	D	1	<input type="checkbox"/>	1->first	2->afternoon	0	test2	Group Verify

8.5 Holidays setting

1. Entered the holidays set. Choose Access Control Settings -> holidays set. Shown as following.

Holiday Setting

No.	Begin date	End date	Time zone
1	05-01	05-03	
2	06-17	06-17	0

New Delete Save

2. Click "New" button to add a new one, The default date is the current day.

No.	Begin date	End date	Time zone
1	05-01	05-03	
2	06-17	06-17	0
3	10-29	10-29	0

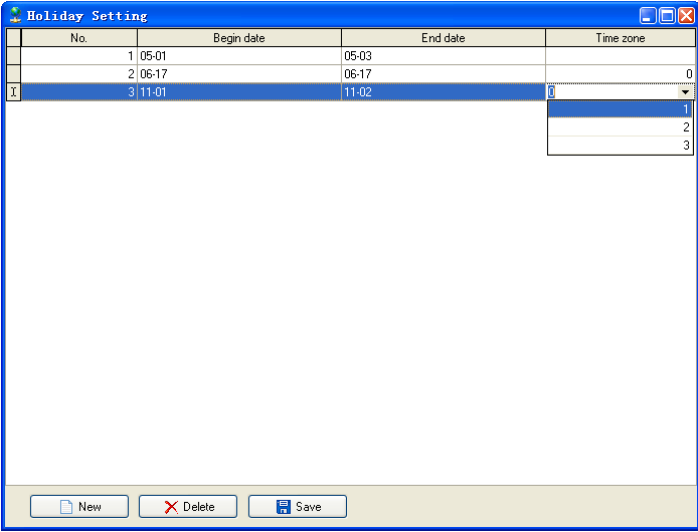
New Delete Save

3. Move cursor to the "Begin date" and "end date" to modify the date.

No.	Begin date	End date	Time zone
1	05-01	05-03	
2	06-17	06-17	0
3	2010-10-29	10-29	0

New Delete Save

4. Moved the cursor to the Time zone to be set, choose the valid Access Control Time zone.



The screenshot shows a window titled "Holiday Setting" with a table and a dropdown menu. The table has four columns: "No.", "Begin date", "End date", and "Time zone". The data in the table is as follows:

No.	Begin date	End date	Time zone
1	05-01	05-03	
2	06-17	06-17	
3	11-01	11-02	0

The dropdown menu for the "Time zone" column of the third row is open, showing the following options:

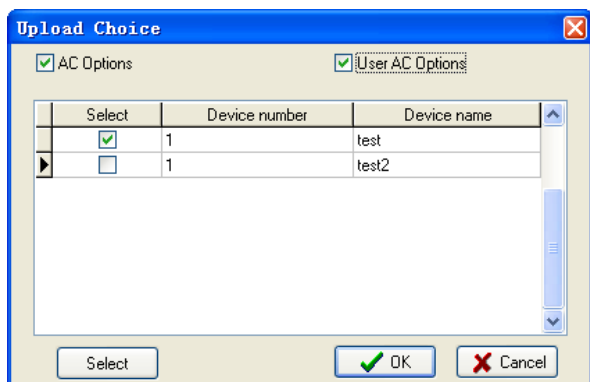
- 0
- 1
- 2
- 3

At the bottom of the window, there are three buttons: "New", "Delete", and "Save".

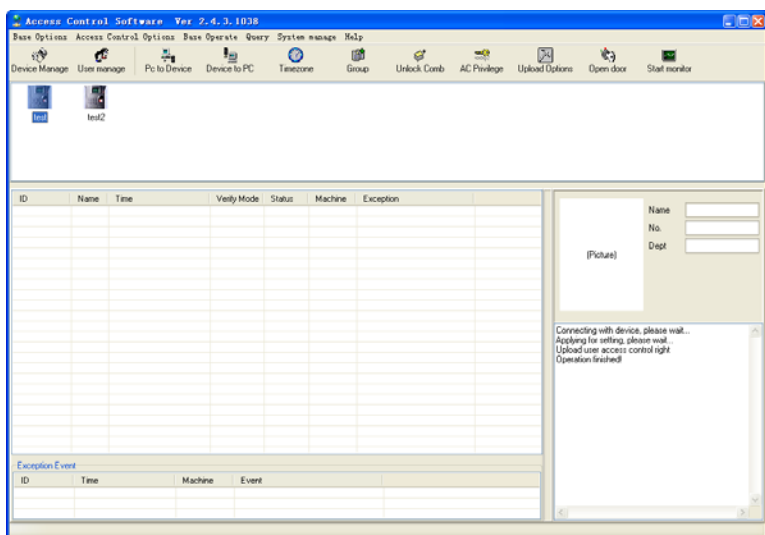
5. Set is completed, click on the "Save" button, the setting will be saved.

8.6 Upload Setting

1. Choose upload device. click icons to choose the device with mouse.



4. Upload success, in its lower right corner the successful operation prompt will be displayed, shown as below.



9. Other Function

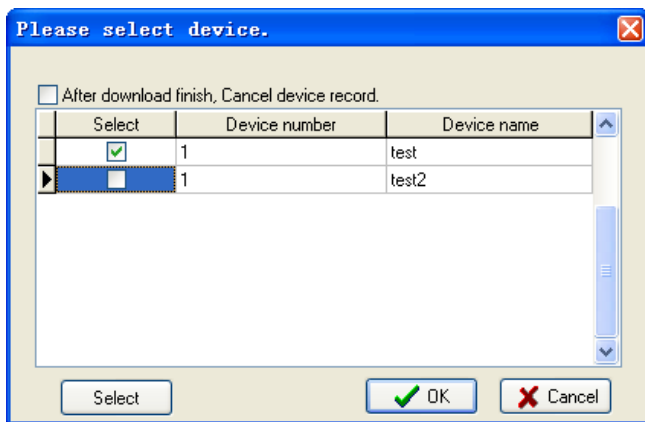
9.1 Start Monitor

You can click the [Start Monitor] button to start system polling and monitoring, and the button changes to [Stop].

When system is in the monitor status, the information about opening door and fingerprint verification will show on the list field.

9.2 Download Log

In the absence of monitor situation, in order to download the system records, you can right click the device, the operation menu appears. Click [Download Log], the dialog popup as below.



Select the device and click [OK] to finish the download process. If you select [After download Finish, Cancel device record], the system will delete the device record when downloading complete.

In monitoring state, if you want to download the device record, click [Download Record] in [Base operate] menu, the system will download all

connected devices' record to system.

9.3 Clear Log

If you want to clear the device record, please right click the device icon, and click [Clear log], the system will prompt the confirm dialog.

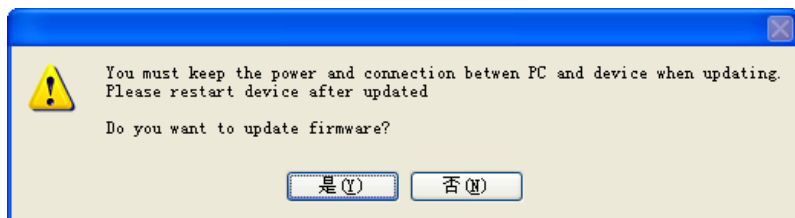
Click [Yes (Y)] to clear the device records.


9.4 Sync Time

If the device time is not synchronizing with the system, please right click the device icon, and click [Sync Time] button.

9.5 Update Firmware

If the device has the older firmware, you can update the firmware by right click the device, and click the [Update Firmware] button. After updating, you need to restart the device. The prompt shown as follow.



 **Notice:** Please do not upgrade the firmware at your discretion because it may bring problems and affect the normal use of the device. Contact our distributors for technical support or upgrade notification.

9.6 Restart Device

If you want to restart the device using the software, please right click the device icon, and click [Restart Device] button to restart it.

9.7 Property

Please right click the device, and click [Property] button in the prompt dialog. Enter the [Device Manage] interface, the specific operation please refer to [4. Device Management](#).

9.8 Stop Sound

After the system alarm has been triggered, right click the device, appears the operation menu, click the [Stop Sound] to stop the system sound and light alarm.

10. Record Management

10.1 Record Query

1. In [Query] down drop menu, you can select [Log query], show as following.

Search Employee's Checking Record

Condition

Time

From: 2010-10-23 00:00

To: 2010-10-29 23:59

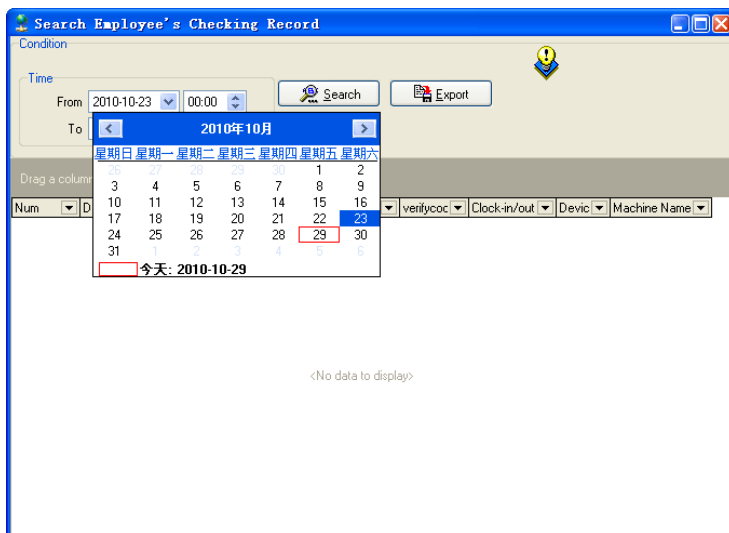
Search Export

Drag a column header here to group by that column

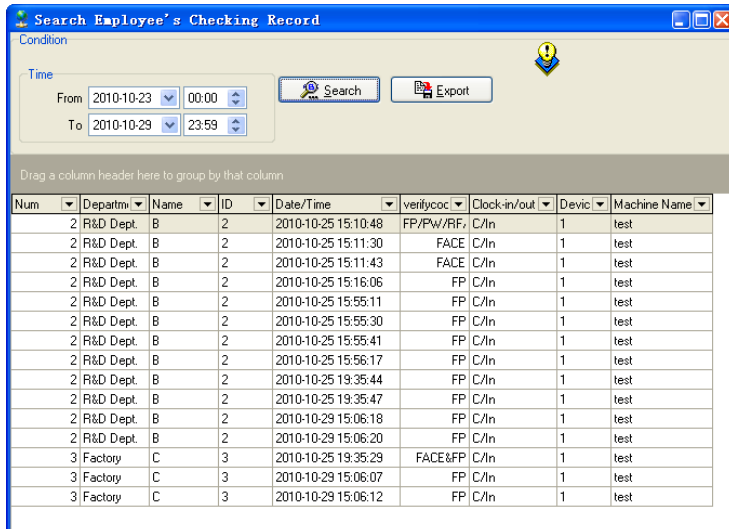
Num	Departmi	Name	ID	Date/Time	verifycoc	Clock-in/out	Devic	Machine Name
<No data to display>								

2. Select the start and end date to query log.

10. Record Management

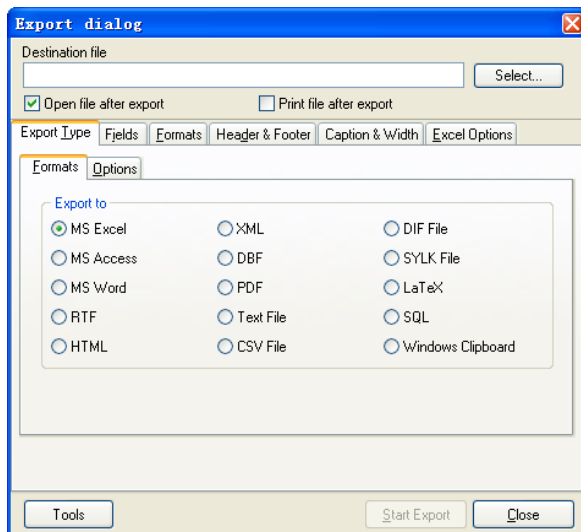


3. Click [Query], the in/out access log within these date will show in the list.



4. Click [Export] to output fingerprint records in various formats, such as

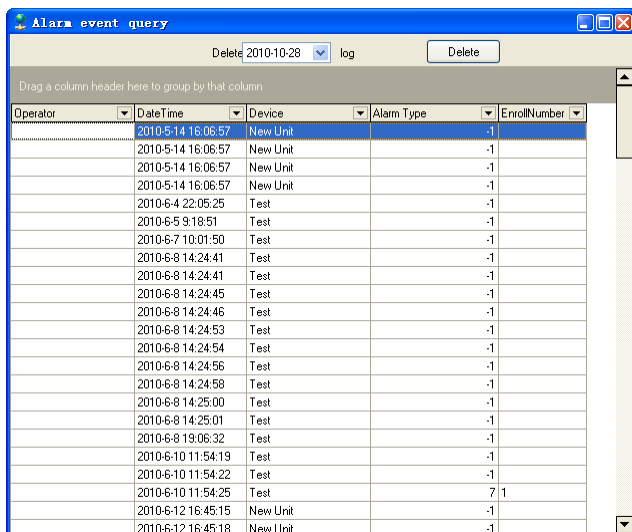
Excel format, etc. this operation is similar to user management exporting.



10.2 Alarm Report

Detect fingerprint that does not pass verification, duress fingerprint, that will trigger the alarm. Click “Alarm event” in the [Query] drop-down menu, and “alarm event query” window will pop up, as shown in the following picture:

10. Record Management



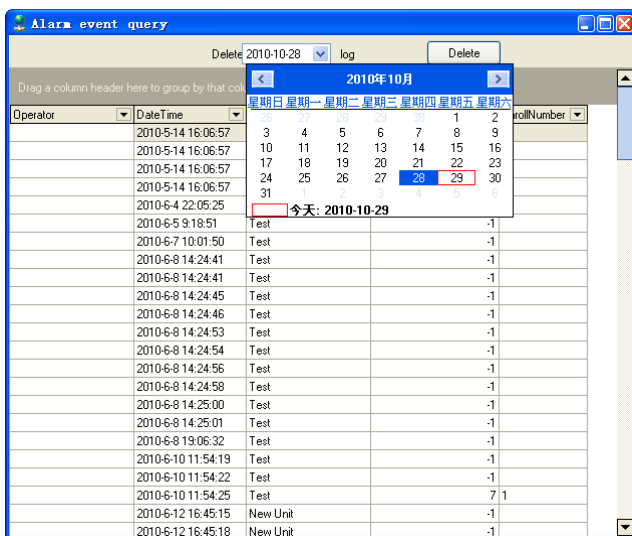
Alarm event query

Delete 2010-10-28 log Delete

Drag a column header here to group by that column

Operator	DateTime	Device	Alarm Type	EnrollNumber
	2010-5-14 16:06:57	New Unit		-1
	2010-5-14 16:06:57	New Unit		-1
	2010-5-14 16:06:57	New Unit		-1
	2010-5-14 16:06:57	New Unit		-1
	2010-6-4 22:05:25	Test		-1
	2010-6-5 9:18:51	Test		-1
	2010-6-7 10:01:50	Test		-1
	2010-6-8 14:24:41	Test		-1
	2010-6-8 14:24:41	Test		-1
	2010-6-8 14:24:45	Test		-1
	2010-6-8 14:24:46	Test		-1
	2010-6-8 14:24:53	Test		-1
	2010-6-8 14:24:54	Test		-1
	2010-6-8 14:24:56	Test		-1
	2010-6-8 14:24:58	Test		-1
	2010-6-8 14:25:00	Test		-1
	2010-6-8 14:25:01	Test		-1
	2010-6-8 19:06:32	Test		-1
	2010-6-10 11:54:19	Test		-1
	2010-6-10 11:54:22	Test		-1
	2010-6-10 11:54:25	Test		7 1
	2010-6-12 16:45:15	New Unit		-1
	2010-6-12 16:45:18	New Unit		-1

Delete alarm event: Select the end date, as following interface.



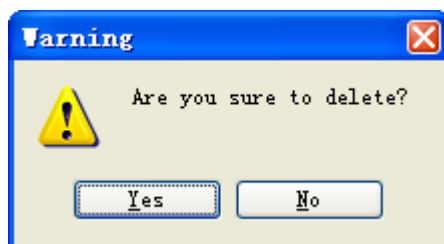
Alarm event query

Delete 2010-10-28 log Delete

Drag a column header here to group by that column

Operator	DateTime	Device	Alarm Type	EnrollNumber
	2010-5-14 16:06:57			-1
	2010-5-14 16:06:57			-1
	2010-5-14 16:06:57			-1
	2010-5-14 16:06:57			-1
	2010-6-4 22:05:25			-1
	2010-6-5 9:18:51	Test		-1
	2010-6-7 10:01:50	Test		-1
	2010-6-8 14:24:41	Test		-1
	2010-6-8 14:24:41	Test		-1
	2010-6-8 14:24:45	Test		-1
	2010-6-8 14:24:46	Test		-1
	2010-6-8 14:24:53	Test		-1
	2010-6-8 14:24:54	Test		-1
	2010-6-8 14:24:56	Test		-1
	2010-6-8 14:24:58	Test		-1
	2010-6-8 14:25:00	Test		-1
	2010-6-8 14:25:01	Test		-1
	2010-6-8 19:06:32	Test		-1
	2010-6-10 11:54:19	Test		-1
	2010-6-10 11:54:22	Test		-1
	2010-6-10 11:54:25	Test		7 1
	2010-6-12 16:45:15	New Unit		-1
	2010-6-12 16:45:18	New Unit		-1

2. Click “Delete” and the following prompt will show:



3. Click [Yes] to delete the events before this date. After that, these events won't show in the list.

11. Appendix

11.1 Common Operation

1. The toolbar for datasheet operation:



The blue bar which locates line is current line in the datasheet. All operation for datasheet is performed on the current line. Only black button is operational, it can not operate when it is gray.

Click button, put it to corresponded operate.



: First, move from the current line to the first line.



: Previous, move from the current line to the previous line.



: Next, move from the current line to the next line.



: Last, move from the current line to the end line.



: Insert, add new record.



: Delete, cancel current record.



: Edit, enter edit status to modify record.



: Save, save the record to be edited.

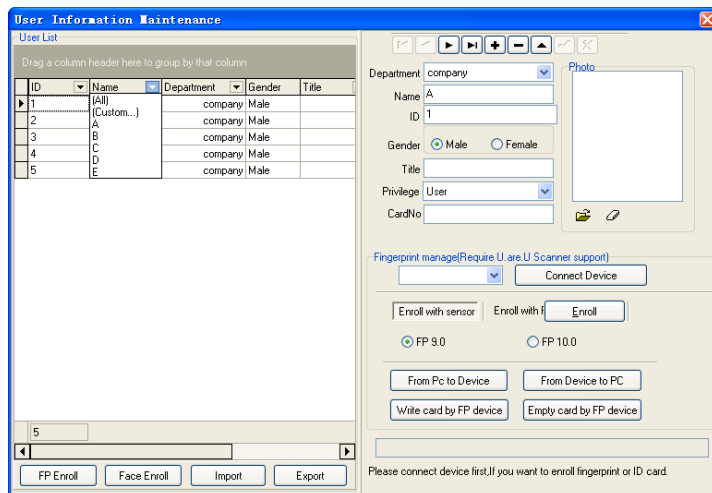


: Cancel Edition, cancel modification for the record.

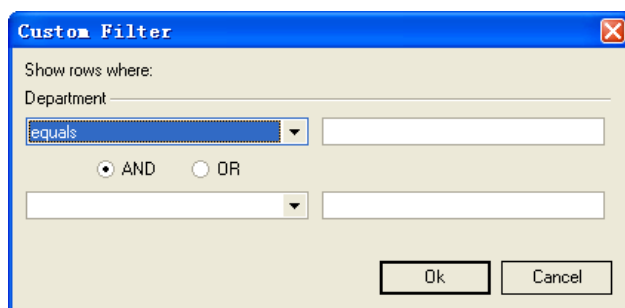
2. Filtrate Data

Filtrate data is that select the record which meet defined condition from the original table sheet, the current display window is following, the operation flow of the filtration data's command.

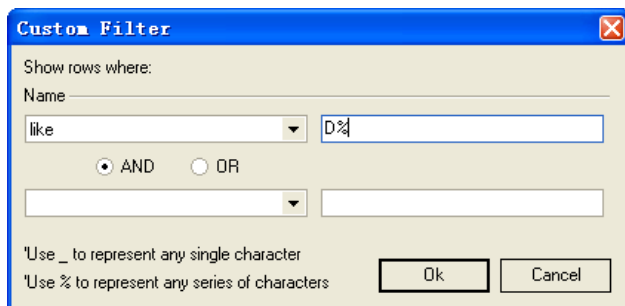
(1) Click down drop menu of the data rank, appear following figure.



(2) Click [Custom Filter], appear following figure.

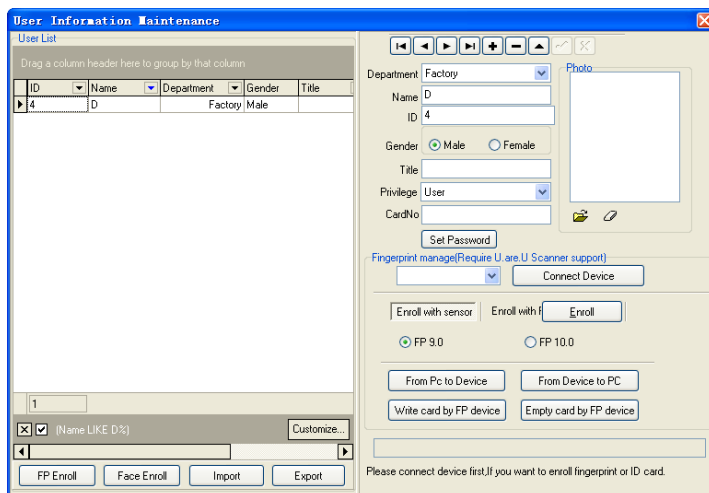


(3) Input condition, such as show all user who's surname is H, appear following figure.



Notice: % must be English symbol. Chinese symbol is rejecting to know.

(4) Click **[OK]**, to show the result of filtration.



☒: Whether do use the filtrate condition.

☒: Cancel filtrate operation.

If you want to cancel current filtration result, display all record, click ☒ or ☒.

3. Record Group

According to a field or multi-field, you can group the record. If you want to

realize group that can draw the rank head to upper side empty part, as the following figure.

11.2 FP, FP device and Card User Guide

The system offer Fingerprint user, Card user, Card and fingerprint multi-user verification.

1. ID Card User

1. Enroll ID card

There are two statuses to enroll ID card.

A. Only Own ID card User

It is suit the user who own the higher privilege or the too poor fingerprint to identify, reference [User Management] part of FP Reader user guide to enroll user, the enroll process is that: Add User → Input User Base Information → Connect to FP Reader with ID card → Wave Card → Save ID Number → Upload User Information.

B. User Verified by FP and Card

It is optimized for the general user, user must enroll the card and fingerprint, there are two ways to verify for user, one is to present the card to identify, the other way is verification fingerprint after waving card near the properly place of the reader. The enroll process is that: Add User → Input User Basic Information → Connect to FP Reader with ID Card → Enroll Fingerprint → Wave Card → Save ID Number → Upload User fingerprint and Information.

2. ID Card User Verification

There are two following verification models for ID card user.

A. Only verification ID card

User only need to wave the registered ID card near to the front of the reader or place the finger on the sensor to match for verification, this verification way is applied to the low security requirement area, but it is easy to use, it is optimized for the officer site which own the high public

security system, reference **[Verification]** part of FP Reader user manual to enroll user, the set process is that: Open **[Equipment Manage]** → Select to be **[Verification]** → Click **[Verification]** → **[Read Options]** → Remark on **[Verification ID Card]** item to **[Yes]** → **[Apply Options]**.

Notice: There are only **[Only verify ID card]** and **[Only 1:1 verify]** to suit ID card setup in the verification option, the **[Register Mifare card only]** is just used for Mifare user. When you set to verify ID card, the **[Only 1:1 verify]** must be remarked as **[NO]**, the **[Register Mifare card only]** is set to read the default.

B. Only 1:1 verify

User must to wave the card near the front of the reader before place the finger on the sensor to verify until it is positive answer. This verification way is applied to the higher security requirement area. It is optimized for a lot of user site, the set process is that: Open **[Equipment Manage]** → Click **[Verification]** → **[Read Options]** → Remark on **[Only verify ID card]** item and **[Only 1:1 verify]** item to **[Yes]** → **[Apply Options]**.

We suggest adopt this verification method when the device store fingerprint up 500, because the more fingerprint there are, the more slowly is device matching speed, the FAR (False Acceptance Rate) will be much more, the Only verify ID card can speed up to identify and keep away fingerprint false acceptance.

2. Mifare Card User

1. Enroll Mifare Card

Please reference **[User Manage]** part of FP Reader user guide to enroll user, the enroll process is that: Add User → Input User Base Information → Connect to Fingerprint Reader with Mifare Card → Use UareU Sensor or FP Reader to enroll fingerprint → Write Card via Fingerprint Reader → Wave Card → Write Card Successfully,

The fingerprint can store in the Mifare card, the result and efficacy of to wave a card is same as to place finger to identify. Select device with Mifare is optimal option for user.

2. Mifare Card Verification Model

There are following verification modal for Mifare card user.

A. Only verify Mifare Card

The same as ID card, it only need to present the card for passing verification, in order strengthen security of the application in the normal condition the item is set as **[NO]**, so and must place the finger to identify after to present a card to verify .

B. Only Verify 1:1

The same as ID card, first must present card and then place the finger on the sensor, if don't present the card, the finger will be reject to accept fingerprint.

Register Mifare card only:

This item set as **[Yes]**, the User ID of Mifare must be store in the reader, otherwise it is fail to pass, if this item set as **[NO]**, it is no need to store user ID in the reader to performance the match.

Fingerprint Card user Table:

Only verify ID Card	Only verify 1:1	User type	Note
Y	Y	Only Card	Only support Card
Y	NO	Card or Fingerprint	Support Card or Fingerprint
NO	Y	Card + Fingerprint	Only support to fingerprint match after to present card
NO	N	Card + Fingerprint	After to present the card to

		or Fingerprint Only	press finger or only to match fingerprint
--	--	---------------------	---

Suggest Select Setup Type:

Version	Name	Only verify ID Card	Only verify 1:1	Note
Standard	Standard Fingerprint Reader	NO	NO	Card + fingerprint or Fingerprint Only
Build In ID	Build in ID Fingerprint Reader	NO	Y	Card + Fingerprint
	Build in ID Fingerprint Reader	NO	Y	Card + Fingerprint
Build in Mifare	Build in IC Fingerprint reader	NO	Y	Card + Fingerprint